The FortiGate Cookbook

& QuickStart Guide

FortiOS 5.2

Register for Support

Register your Fortinet product to receive:
- Technical Support
- New product features
- Protection from new threats

Vous devez enregistrer le produit pour recevoir:
- Support technique
- Nouvelles fonctionnalités du produit
- Protection contre de nouvelles menaces

La reistrazione ti permette di usufruire di:
- Supporto Tecnico
- Nuove funzionalita
- Proteezione dalle ultime minaccce

Debe registrar el producto para recibir:
- Apoyo técnico
- Nuevas funcionalidades del producto
- Protección contra ataques

登録のお願い
本日、フォーティネット製品の登録をしてください。
登録すると次のメリットがあります。
テクニカルサポート・新機能の追加・新しい脅威への防御

请马上注册
您的飞塔产品
您在注册以后才能得到技术支持、新产品特点信息、最新威胁防护

http://forti.net/support
Toll free: 1 866 648 4638
Phone: 1 408 486 7899
Fax: 1 408 235 7737
Email: register@fortinet.com

The FortiGate Cookbook & QuickStart Guide 5.2

June 15, 2015
01-520-250472-20150615

Device Guide

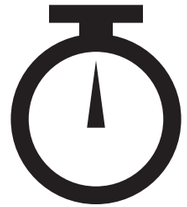
http://forti.net/docs/fortigate

Included Accessories List

Port Guide

LED Guide

Mounting Guide



1 FortiGate Setup

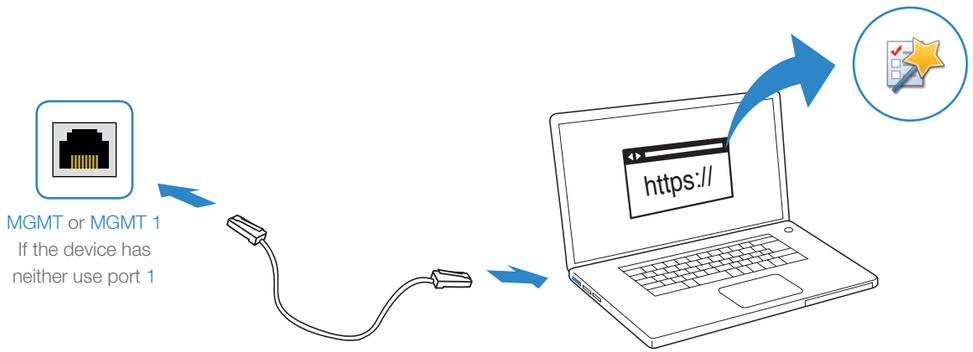
- A **Web browser** — Setup Wizard
- B **Windows/OS X** — with FortiExplorer
- C **Terminal emulation** — with console cable
- D **iOS** — FortiExplorer app configuration

2 SFP Tranceivers

- A **Installation**
- B **Removal**

1 FortiGate Setup

A Web Browser with Ethernet Cable



To Connect to the GUI

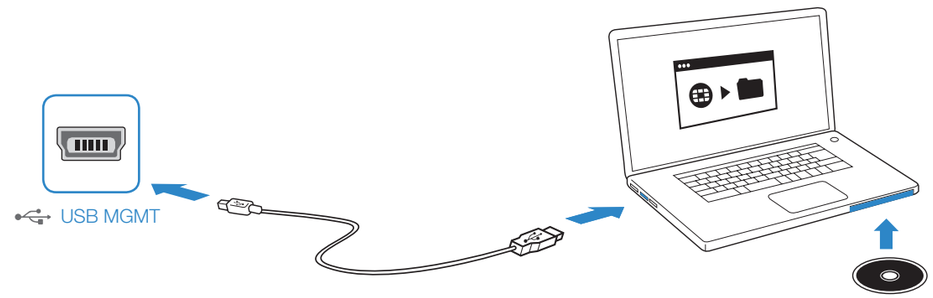
1. Connect the Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface as the FortiGate unit:

   IP address: 192.168.1.XXX
   Netmask: 255.255.255.0

3. Visit 192.168.1.99 in your web browser.
4. Login using username "admin" and no password.
5. Configure your device and save your settings.
6. Register your device from the dashboard page.

B Windows/OS X with USB

FortiExplorer provides direct access to your FortiGate configuration without modifying your network settings. Other features and tools include: automatic firmware downloads, easy registration, and access to additional device resources.



1. Install FortiExplorer from the included CD or download it from http://forti.net/fexp.

Microsoft Windows Install

2. Connect the USB cable and launch FortiExplorer if it does not launch automatically.

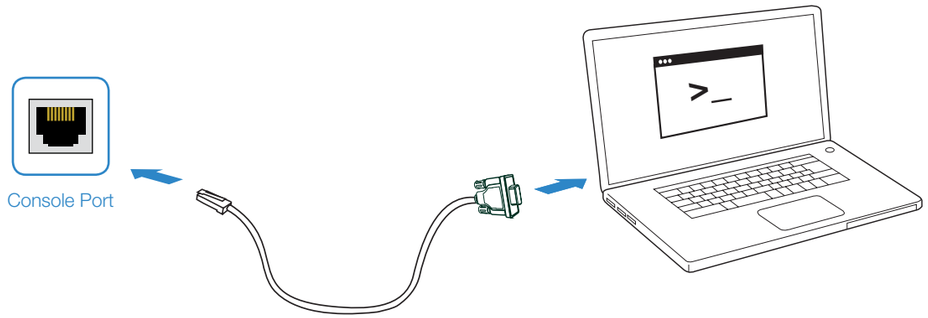
Mac OS X Install

2. Open the .dmg file and drag the FortiExplorer icon to the Applications folder.
3. Connect the USB cable.
4. Open the FortiExplorer icon to launch the application.

FortiExplorer Setup Wizard

1. Follow the prompts or click "Register" to register your device with FortiCare.
2. Click "Setup Wizard".
3. Log in using username "admin" and no password.
4. Follow the steps to the Setup Wizard steps.
5. Click "Configure" to complete the setup of your device.

C Terminal Emulation with Console Cable



To Connect to the Command Line Interface (CLI)

1. Connect the FortiGate unit console port to the management computer using the provided console cable.
2. Start a terminal emulation program on the management computer, select the appropriate COM port, and use the following settings:

Baud rate: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

3. Press Enter on your keyboard to connect to the CLI.

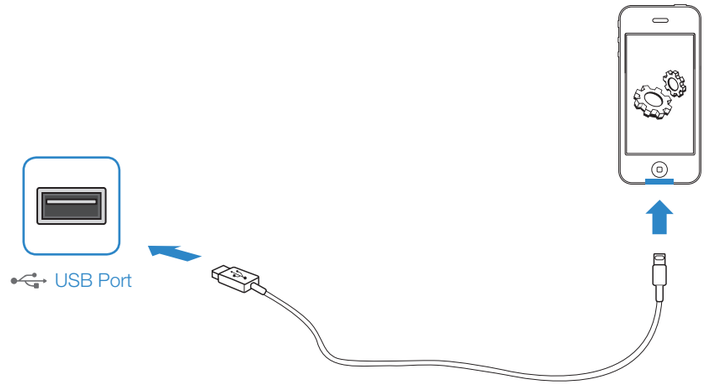
```
FortiGate # ?
config      Configure object.
get         Get dynamic and system information.
show        Show configuration.
diagnose    Diagnose facility.
execute     Execute static commands.
exit        Exit the CLI.

FortiGate # config ?
alertemail              Alert email configuration.
antivirus               AntiVirus configuration.
application             Application control configuration.
client-reputation       Client reputation tracking configuration
dlp                     DLP configuration.
endpoint-control        Endpoint control configuration.
firewall                Firewall configuration.
ftp-proxy               FTP proxy configuration.
gui                     GUI configuration.
icap                    ICAP client configuration.
imp2p                   IM & P2P policy configuration.
ips                     IPS configuration.
--More--
```

4. Log in using username “admin” and no password. You can now proceed with configuring your FortiGate unit.

Get started by typing “?” for a list of available commands.
Begin typing a command and type “?” for a list of available ways to complete the command.
For example “config ?” will show the lowest level of configuration options.

For a detailed guide visit http://forti.net/cli.

D iOS with Apple to USB Cable



FortiExplorer App

1. Download the FortiExplorer iOS App to your device from http://forti.net/fexp-ios.
2. Use your Apple to USB cable to connect to the FortiGate unit’s USB port.
3. Launch the FortiExplorer App and select your device model.
4. Log in using username “admin” and no password.
5. Configure your device.

Available on the App Store

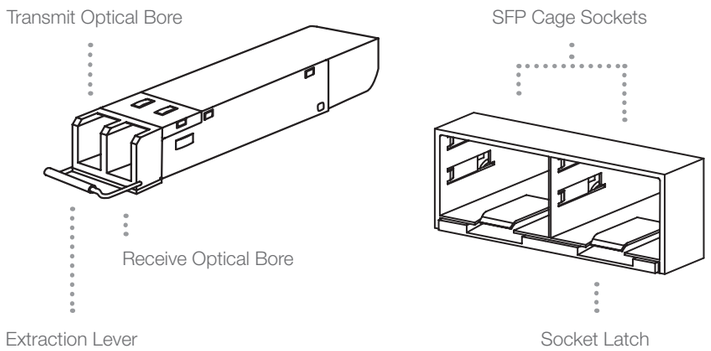
http://forti.net/fexp-ios

2 SFP Transceivers

Caution:
SFP transceivers are static sensitive devices. Use an ESD wrist strap or similar grounding device when handling transceivers.

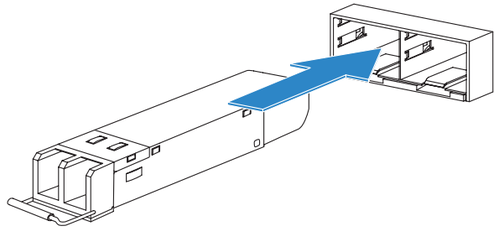
Do not install or remove SFP transceivers while fiber-optic cables are still attached. This can cause damage to the cables, cable connectors, and the optical interfaces. It may also prevent the transceiver from latching correctly into the socket connector.

Do not force the SFP transceivers into the cage slots. If the transceiver does not easily slide in and click into place, it may not be aligned correctly or may be upside down. If this happens, remove the SFP transceiver, realign it or rotate it and slide it in again.



A Installation

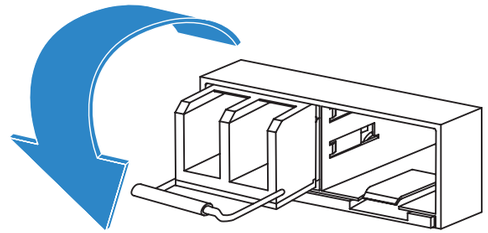
1. Ensure that you are properly grounded.
2. Remove the cap from the SFP cage socket on the front panel of the unit.
3. Position the SFP transceiver in front of the cage socket opening and ensure that the transceiver is correctly oriented. When the transceiver is correctly oriented, the extraction lever will be level with the socket latch.
   Note: SFP cage socket orientation may vary. Ensure that the SFP transceiver is correctly oriented each time that you are inserting a transceiver.
4. Hold the sides of the SFP transceiver and slide it into the cage socket until it clicks into place.



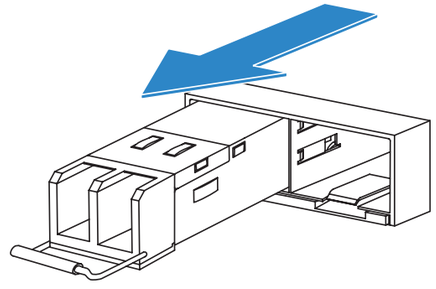
5. Press the transceiver firmly into the cage socket with your thumb.
6. Verify that the transceiver is latched correctly by grasping the sides of the transceiver and trying to pull it out without lowering the extraction lever.
   If the transceiver cannot be removed, it is installed and latched correctly.
   If the transceiver can be removed, reinsert it and press harder with your thumb.
   If necessary, repeat this process until the transceiver is securely latched into the cage socket.

B Removal

1. Ensure that you are properly grounded.
2. If applicable, disconnect the fiber-optic cable from the transceiver connector and install a clean dust plug in the transceiver's optical bores.
3. Pull the extraction lever out and down to eject the transceiver. If you are unable to use your finger to open the lever, use a small flat-head screwdriver or other similar tool to open the lever.



4. Hold the sides of the transceiver and carefully pull it away from the cage socket.

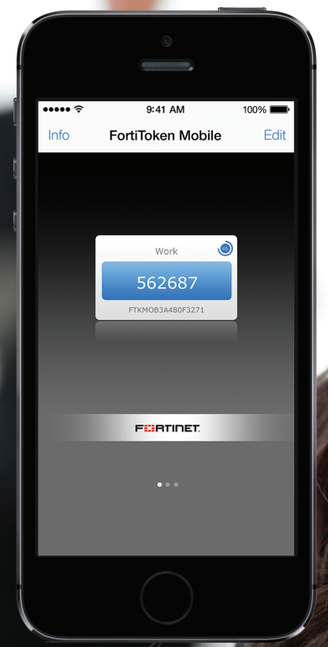


5. Replace the cap on the SFP cage socket and place the removed SFP transceiver into an antistatic bag.

Note:
Installing and removing SFP transceivers can shorten their useful life. Do not install or remove transceivers more than is necessary.

Follow proper fiber-optic handling procedures when installing and removing SFP transceivers to ensure that the devices remain clean and are not damaged.

Free Licenses & Services for FortiCare Registered FortiGates



Stay extra secure by using your phone as second-factor authentication for remote administration. Get extra tokens from your reseller.

2 FortiToken Mobile Licenses

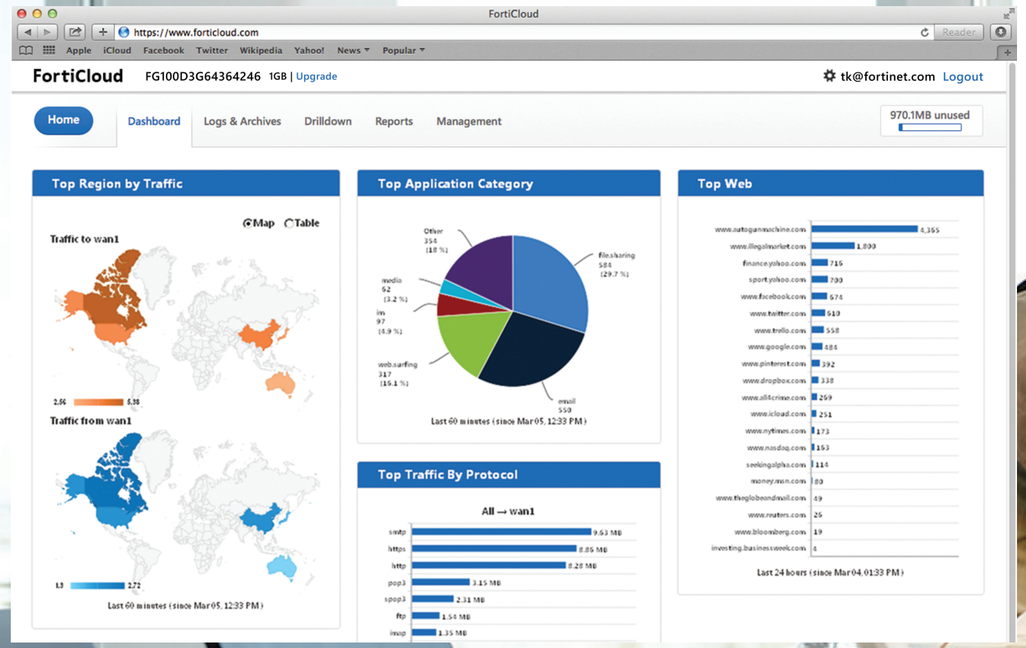
Manage security on your endpoints. Keep your network clean and allow employees to bring devices. Add more client licenses via your reseller.

10 FortiClient Endpoint Licenses

Make remote access simple. Use yourcompany.fortiddns.com instead of hard-to-remember or changing IP addresses.

Fortinet DDNS Service

Free Licenses & Services for FortiCare Registered FortiGates



Generate reports, backup configurations and more with an easy-to-use cloud based portal.

FortiCloud 1GB

Services Included with FortiCare Subscriptions

FortiCare is global 24/7 support for your Fortinet hardware & software

Get the latest product security updates and features. Stay with us and see the product evolve.

Firmware Updates

Use cellphone technology as backup Internet connection. We are always adding support for new third party 3G/4G + devices.

USB Modem Database Updates

Setup policies and track activities based on geography. Your FortiGate will intelligently identify where an IP is originated or destined.

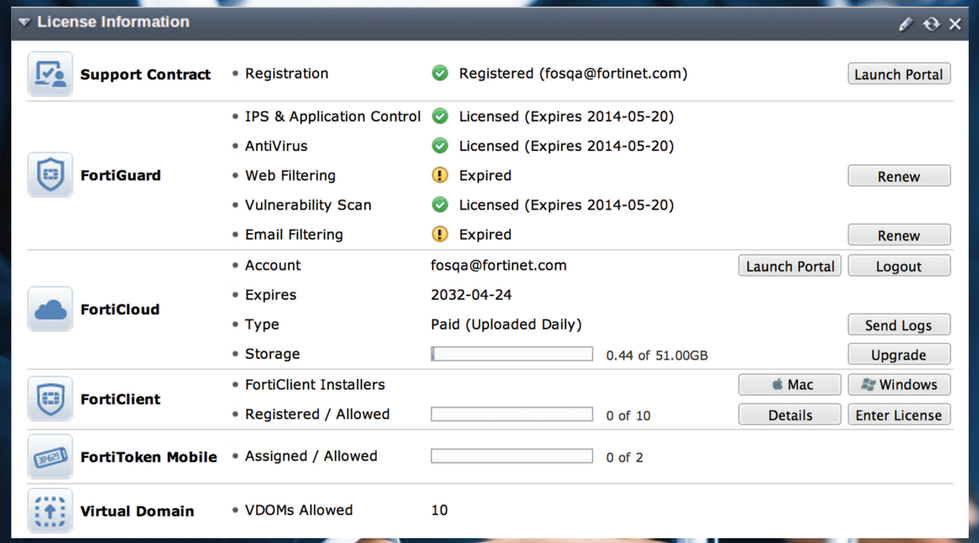
Geo-IP Database Updates

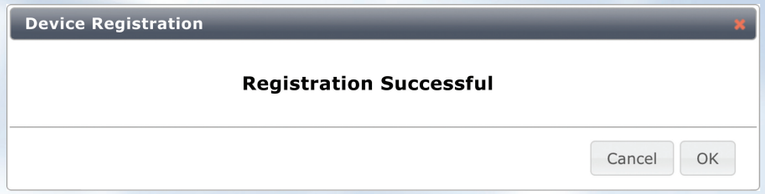
Identify device type and OS information. Great for organizations that allow employees to bring in devices and want to enforce device based policies.

Device Signatures Database Updates

First Day with FortiOS

Here are some things you can do to get started with the power and simplicity of FortiOS





1 Register and Check Services

Make sure you are registered. This will ensure that your device is protected against the latest threats.

Once this is done, check to ensure all your purchased services are enabled by visiting the Dashboard. Contact your Fortinet partner if you experience any issues.

2 Run Through the Setup Wizard

Be guided through simple steps to immediately setup most important features.

3 Setup a Backup Cellular Connection

Use a 3G or 4G modem as a backup or alternate Internet connection. The Setup Wizard will walk you through this. If you are unable to get a cellphone connection at the location of your FortiGate, purchase a FortiExtender.

4 Create a WiFi Network

Reduce cabling in your office with a FortiWifi or FortiAP attached to a regular FortiGate.

After attaching a FortiAP, click WiFi Controller > Managed Access Points > Managed FortiAPs and enable the detected AP by clicking Edit then Allow.

5 Customize Your Firewall

Prevent incoming and outgoing traffic to the requirements of your organization.
Click Policy > Policy and Create New.

6 Setup Remote Access

Securely link one office to another, or allow employees access essential resources from locations outside the office.
VPN > Create VPN Wizard.

7 Checkout All the Support

http://forti.net/docs has a huge range of documents to help you through every scenario.

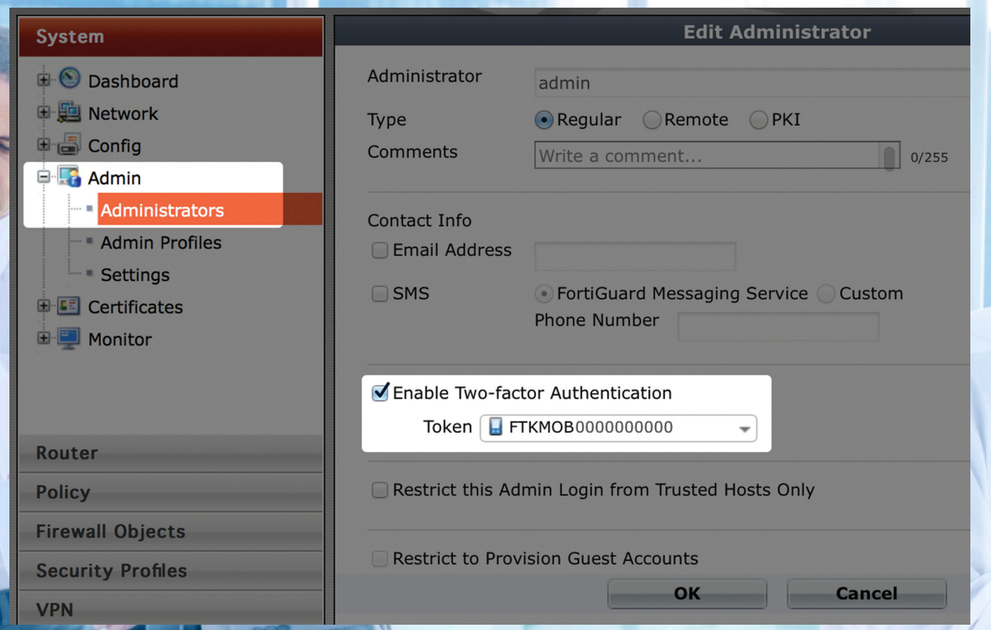
8 Feel the Power

Your FortiGate is using components you won't see anywhere else. Most devices use a standard CPU that is good at most things but great at none.

Within your device is a unique SoC (System on a Chip) that combines several security-focused technologies designed by Fortinet. While our most powerful products have dedicated CP (Content Processors) and NP (Network Processors), our desktop models share all the groundbreaking technological discoveries at a great price and small form factor.

Licenses & Subscriptions

Day Two with FortiOS



1 Use Mobile Tokens to Double Your Security

Android and iOS devices can be used as second factor authentication. This means that someone attempting to administer the device will need both your mobile device and your password to be able to login.

Two mobile tokens are provided no-charge with your device. Please ensure that you have registered your FortiGate to enable them.

To start with, you might want to add a secondary Admin account for yourself to use remotely. It will be more secure if you use a mobile token with it.

Click Admin > Administrators from the left menu, select an administrator and Edit to configure the mobile token.

Users can also be assigned tokens. Users and Devices > Users select a user and Edit to configure the mobile token.

2 Get Those 'Nice to Haves' Working

The FortiGate Cookbook is an excellent resource for a quick walkthrough on features you didn't think you had time to setup.

3 Allow Personal Devices on Your Network (BYOD)

Install FortiClient on Android, Windows and iOS devices. Each instance of FortiClient can connect to the FortiGate and self-install the security settings you require. Download from FortiClient.com and take a look at profile settings under User & Device > Endpoint Protection > FortiClient Profiles.

4 Expand Your Wired Network

Use a FortiSwitch to maintain complete visibility and control of the network regardless of how users connect devices.

5 Start Monitoring

Once FortiCloud is enabled you can start monitoring your bandwidth usage and analyzing traffic logs. Create reports and send them in scheduled updates to those that want to be in-the-know.

Related Products

FortiManager

Deploy thousands of FortiGates, distribute updates, or install security policies across managed assets.

FortiManager 300D

FortiAnalyzer

Network security logging, analysis, and reporting. Securely aggregate data from your FortiGates.

FortiAnalyzer 300D

FortiExtender

Transmit a 3G/4G connection from the best location on your premise to your FortiGates as backup or primary WAN.

FortiAP

Setup WiFi networks with as many access points as you need. Manage them with your FortiGate.

FortiVoice

Complete control of your business telephone communications. Easy to use, affordable and reliable.

FortiVoice Telephone System

Handset

Introducing FortiSwitch Series

FortiSwitch 224B-POE

FortiFone

FortiCam

FortiAP

Know Your Network

With a FortiSwitch, you can easily identify, monitor and manage all your devices, directly from your FortiGate

FortiSwitch Secure Access series of Ethernet LAN switches deliver outstanding network security, performance and manageability for threat conscious small to mid-sized businesses, distributed enterprises and branch offices.

- Authenticate and monitor specific devices
- Up to 48 ports in a compact 1U form factor
- PoE capable

“Working with Fortinet, Verizon Business is giving customers an all-in-one solution that eases the burden associated with managing the complex security risks of the extended enterprise.”

- Kerry Bailey, Vice President
Verizon Business Security Solutions

Power over Ethernet (PoE) saves the need for addtional electrical wiring. Great for telephones and security cameras. Many FortiGates and FortiSwitches have a PoE option.

Datacenter

Supercharge network segmentation with of 100 Gbps firewall performance

FortiGate-1000 to 3000 series
High speed interfaces.
Powered by multiple NP6 network processors

Branch Office

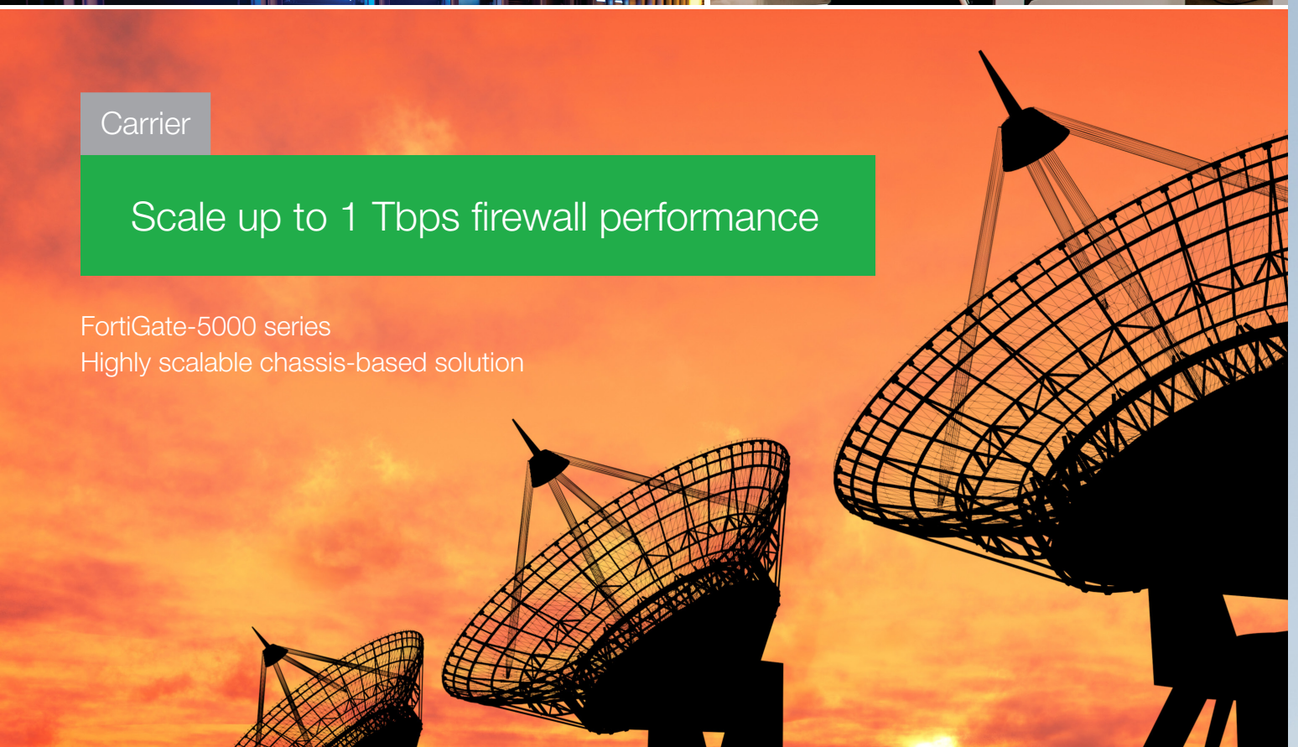
Consolidate network security for lower TCO

FortiGate-100 and 200 series
High port density and PoE variants

Carrier

Scale up to 1 Tbps firewall performance

FortiGate-5000 series
Highly scalable chassis-based solution



Mid Enterprise

Power up security for Internet access

FortiGate-300 to 800 series
Compact. Superior price and performance.
Powered by the latest Fortinet ASIC network processor, the NP6

Corporate Overview

Forward looking market leadership

Fortinet pioneered an innovative, high performance network security solution. We address the fundamental problems of an increasingly bandwidth-intensive network environment and a more sophisticated IT threat landscape. We are a leading provider of network security appliances and the leader in Unified Threat Management, or UTM solutions.

Fortinet is a worldwide leading provider of UTM appliances, with a 16% year over year growth in the UTM security appliance market according to IDC Q3 2013.

IDC
Analyze the Future

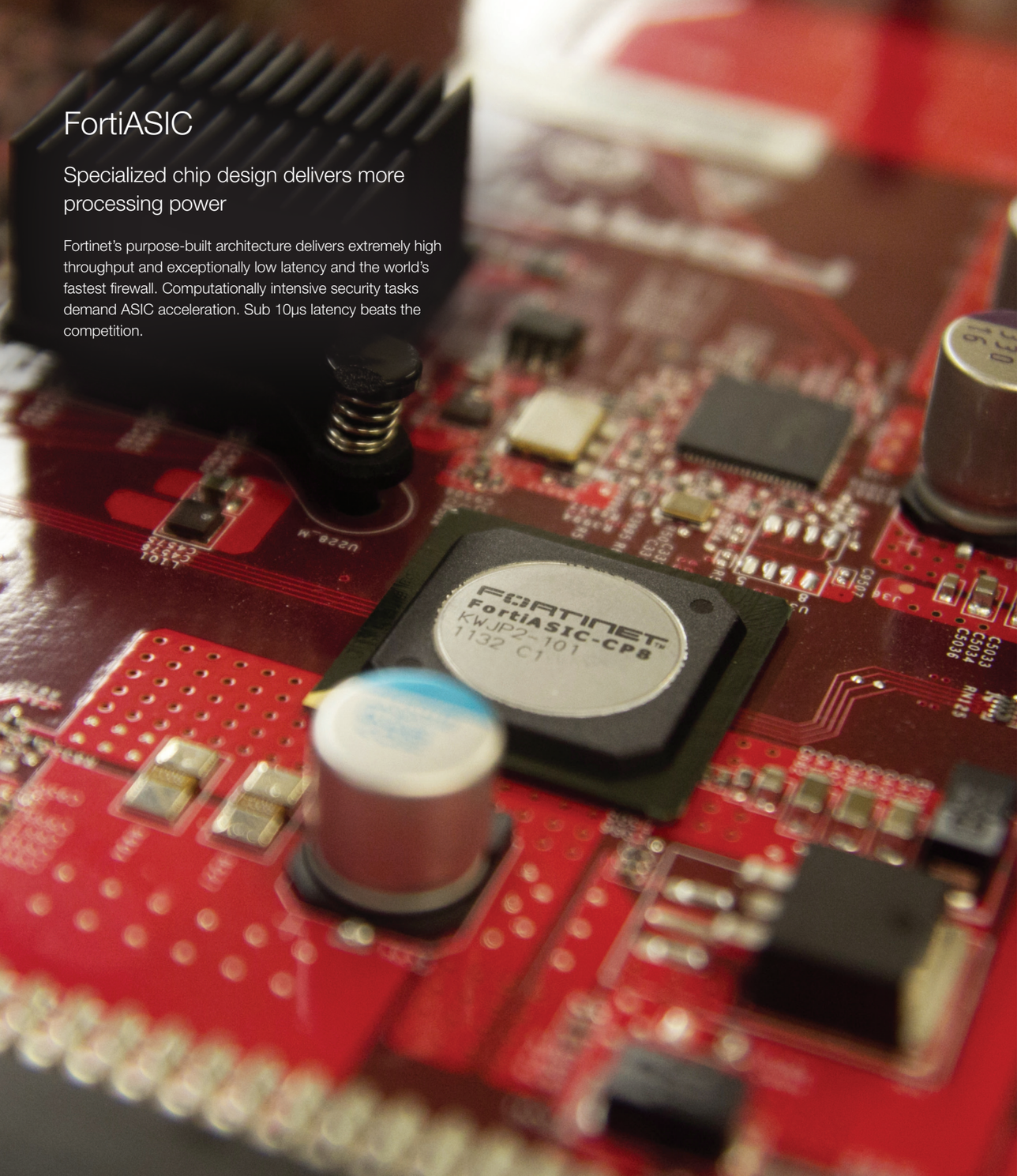
Most Certified in the Industry

Fortinet is the only network security vendor to earn independent certifications across all core security technologies

Fortinet demonstrates our ability to consolidate multiple security technologies while still meeting the highest standards of performance and accuracy.

COMMON CRITERIA EAL4+ CERTIFIED · NSS approved · vb 100 VIRUS virusbtn.com · READY

ICSA labs CERTIFIED FIREWALL - CORPORATE · ICSA labs CERTIFIED NETWORK IPS · ICSA labs CERTIFIED SSL VPN · ICSA labs CERTIFIED ANTI-VIRUS



FortiASIC

Specialized chip design delivers more processing power

Fortinet's purpose-built architecture delivers extremely high throughput and exceptionally low latency and the world's fastest firewall. Computationally intensive security tasks demand ASIC acceleration. Sub 10µs latency beats the competition.

The FortiGate Cookbook

Contents

Introduction

The FortiGate Cookbook provides examples, or recipes, of basic and advanced FortiGate configurations to administrators who are unfamiliar with the unit. All examples require access to the graphical user interface (GUI), also known as the web-based manager.

Each example begins with a description of the desired configuration, followed by step-by-step instructions. Some topics include extra help sections, containing tips for dealing with some common challenges of using a FortiGate unit.

Using the FortiGate Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

Additional recipes and resoures can be found at cookbook.fortinet.com.

This edition of the FortiGate Cookbook was written using FortiOS 5.2.1

Tips for using the Cookbook

Before you get started, here are a few tips about using the FortiGate Cookbook:

Understanding the basics

Some basic steps, such as logging into your FortiGate, are not included in most recipes. This information can be found in the QuickStart guide for your product.

Screenshots vs. text

The FortiGate Cookbook uses both screenshots and text to explain the steps of each example. The screenshots display the entire configuration, while the text highlights key details (i.e. the settings that are strictly necessary for the configuration) and provides additional information. To get the most out of the FortiGate Cookbook, start with the screenshots and then read the text for more details.

Model and firmware

GUI menus, options, and interface names may vary depending on the FortiGate model you are using and the firmware build. For example, the menu **Router > Static > Static Routes** is not available on some models. Also, on different models, the Ethernet interface that would normally connect to the Internet could be named port1, wan1, wan2, or external.

Also, some features are only available through the CLI on certain FortiGate models, generally the desktop models (FortiGate/WiFi-20 to 90 Series).

FortiGate ports

The specific ports being used in the documentation are chosen as examples. When you are configuring your FortiGate unit, you can substitute your own ports, provided that they have the same function.

For example, in most recipes, wan1 is the port used to provide the FortiGate unit with access to the Internet. If your FortiGate uses a different port for this function, you should use that port where the recipe configure uses wan1.

IP addresses and object names

IP addresses are sometimes shown in diagrams to make it easier to see the source of the addresses used in the recipe. When you are configuring your FortiGate unit, substitute your own addresses. You should also use your own names for any objects, including user accounts, that are created as part of the recipe. Make names as specific as possible, to make it easier to determine later what the object is used for.

IPv4 vs IPv6

Most recipes in the FortiGate Cookbook use IPv4 security policies. However, the majority of them could also be done using IPv6 policies. If you wish to create an IPv6 policy, go to **Policy & Objects > Policy > IPv6**.

Turning on features

Some FortiOS features can be turned off, which means they will not appear in the GUI. If an option required for a recipe does not appear, go to **System > Config > Features** and make sure that option is turned on.

Also, on some FortiGate models, certain features are only available using the CLI. For more information about this, see the Feature/Platform Matrix.

Text elements

Bold text indicates the name of a GUI field or feature. When required, italic text indicates information that you must enter.

QR Codes

When a video version of a recipe is available, a QR code can be found at the end of the recipe. This code can be scanned with a mobile device to open the video for playback, provided your device has Internet access using either WiFi or cellular data.

Selecting OK/Apply

Always select OK or Apply when you complete a GUI step. Because this must be done frequently, it is an assumed step and is not included in most recipes.

Choosing your FortiGate's switch mode

This section contains information to help you determine which internal switch mode your FortiGate should use, a decision that should be made before the FortiGate is installed.

What is the internal switch mode?

The internal switch mode determines how the FortiGate's physical ports are managed by the FortiGate. The two main modes are Switch mode and Interface mode.

What are Switch mode and Interface mode and why are they used?

In Switch mode, all the internal interfaces are part of the same subnet and treated as a single interface, called either **lan** or **internal** by default, depending on the FortiGate model. Switch mode is used when the network layout is basic, with most users being on the same subnet.

In Interface mode, the physical interfaces of the FortiGate unit are handled individually, with each interface having its own IP address. Interfaces can also be combined by configuring them as part of either hardware or software switches, which allow multiple interfaces to be treated as a single interface. This mode is ideal for complex networks that use different subnets to compartmentalize the network traffic.

Which mode is your FortiGate in by default?

The default mode that a FortiGate starts in varies depending on the model. To determine which mode your FortiGate unit is in, go to **System > Network > Interfaces**. Locate the **lan** or **internal** interface. If the interface is listed as a **Physical Interface** in the **Type** column, then your FortiGate is in Switch mode. If the interface is a **Hardware Switch**, then your FortiGate is in Interface mode.

How do you change the mode?

If you need to change the mode your FortiGate unit is in, first make sure none of the physical ports that make up the **lan** or **internal** interface are referenced in the FortiGate configuration. Then go to **System > Dashboard > Status** and enter either of the following commands into the **CLI Console**:

1. Command to change the FortiGate to switch mode:

```
config system global
   set internal-switch-mode switch
end
```

2. Command to change the FortiGate to interface mode:

```
config system global
   set internal-switch-mode interface
end
```

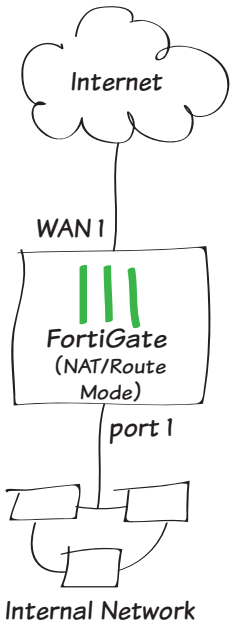
Installing a FortiGate in NAT/Route mode

In this example, you will learn how to connect and configure a new FortiGate unit in NAT/Route mode to securely connect a private network to the Internet.

In NAT/Route mode, a FortiGate unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT).

If you have not already done so, ensure that your FortiGate is using the correct internal switch mode. For more information, see "Choosing your FortiGate's switch mode" on page 3.

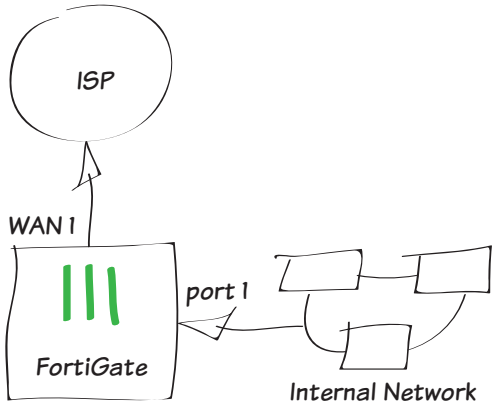
1. Connecting the network devices and logging onto the FortiGate
2. Configuring the FortiGate's interfaces
3. Adding a default route
4. (Optional) Setting the FortiGate's DNS servers
5. Creating a policy to allow traffic from the internal network to the Internet
6. Results



1. Connecting the network devices and logging onto the FortiGate

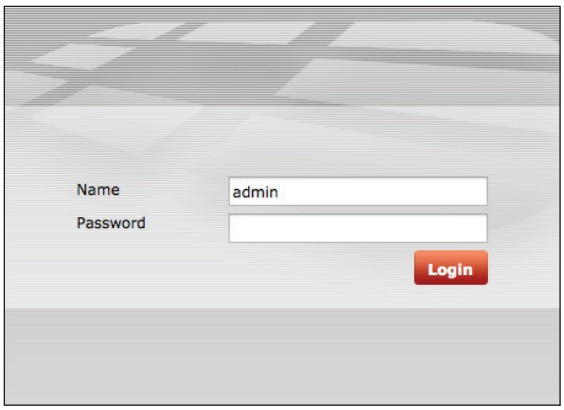
Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment and Connect a PC to the FortiGate using an internal port (typically port 1).

Power on the ISP's equipment, the FortiGate unit, and the PC on the internal network.



From the PC on the internal network, connect to the FortiGate's web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models QuickStart Guide).

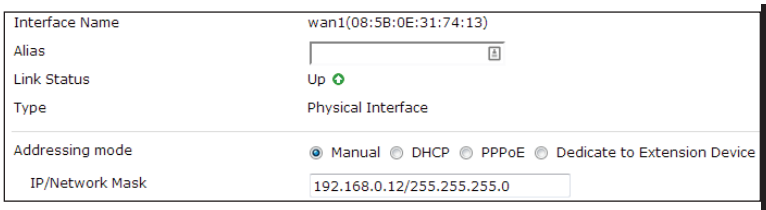
Login using an admin account (the default admin account has the username admin and no password).



2. Configuring the FortiGate's interfaces

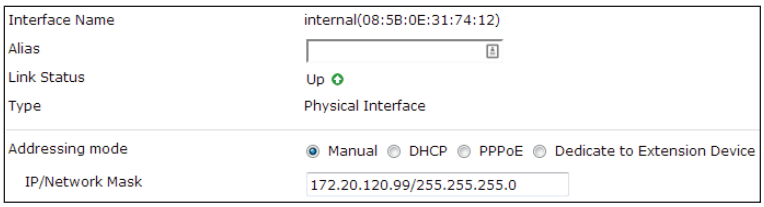
Go to **System > Network > Interfaces** and edit the Internet-facing interface.

Set **Addressing Mode** to **Manual** and the **IP/Netmask** to your public IP address.



Edit the **internal** interface (called **lan** on some FortiGate models).

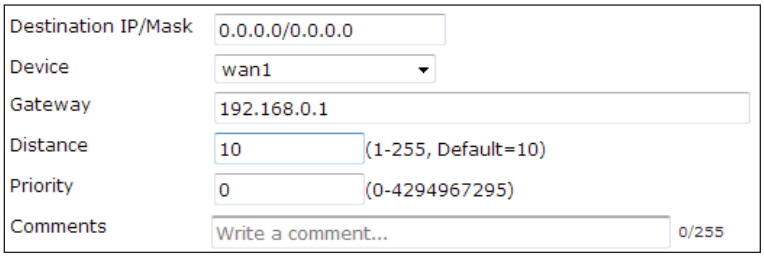
Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate.



3. Adding a default route

Go to **Router > Static > Static Routes** (or **System > Network > Routing**, depending on your FortiGate model) and create a new route.

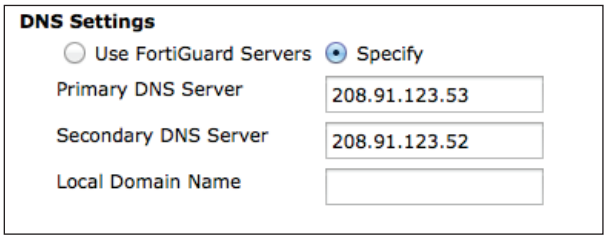
Set the **Destination IP/Mask** to 0.0.0.0/0.0.0.0, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.



A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can edit it or delete it and add a new one.

4. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** servers.



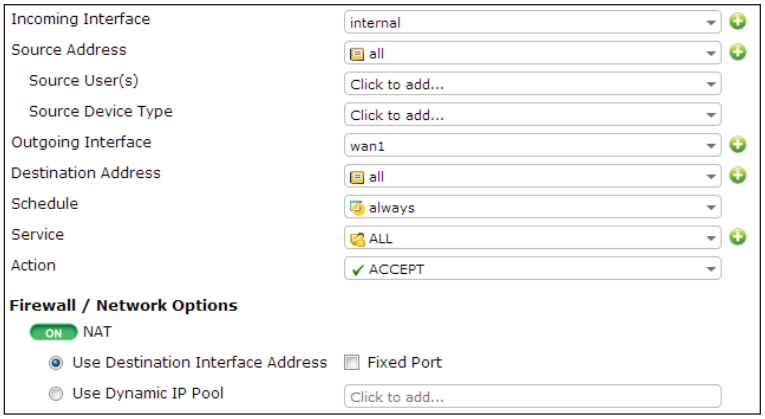
5. Creating a policy to allow traffic from the internal network to the Internet

Some FortiGate models include an IPv4 security policy in the default configuration. If you have one of these models, edit it to include the logging options shown below, then proceed to the results section.

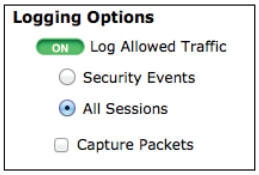
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the **internal** interface and the **Outgoing Interface** to the Internet-facing interface.

Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

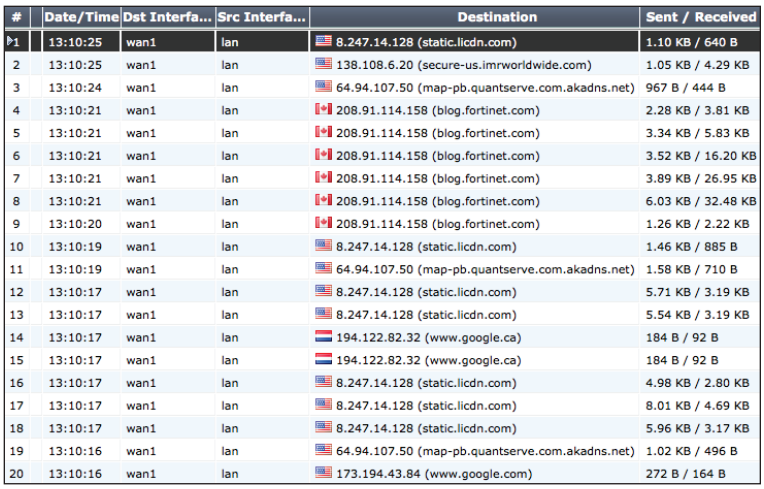


6. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has the **internal** interface as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

If these two columns are not shown, right-click on the title row, select **Src Interface** and **Dst Interface** from the dropdown menu, and then select **Apply**.



#	Date/Time	Dst Interfa...	Src Interfa...	Destination	Sent / Received
1	13:10:25	wan1	lan	8.247.14.128 (static.licdn.com)	1.10 KB / 640 B
2	13:10:25	wan1	lan	138.108.6.20 (secure-us.imrworldwide.com)	1.05 KB / 4.29 KB
3	13:10:24	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	967 B / 444 B
4	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	2.28 KB / 3.81 KB
5	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.34 KB / 5.83 KB
6	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.52 KB / 16.20 KB
7	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.89 KB / 26.95 KB
8	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	6.03 KB / 32.48 KB
9	13:10:20	wan1	lan	208.91.114.158 (blog.fortinet.com)	1.26 KB / 2.22 KB
10	13:10:19	wan1	lan	8.247.14.128 (static.licdn.com)	1.46 KB / 885 B
11	13:10:19	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	1.58 KB / 710 B
12	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.71 KB / 3.19 KB
13	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.54 KB / 3.19 KB
14	13:10:17	wan1	lan	194.122.82.32 (www.google.ca)	184 B / 92 B
15	13:10:17	wan1	lan	194.122.82.32 (www.google.ca)	184 B / 92 B
16	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	4.98 KB / 2.80 KB
17	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	8.01 KB / 4.69 KB
18	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.96 KB / 3.17 KB
19	13:10:16	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	1.02 KB / 496 B
20	13:10:16	wan1	lan	173.194.43.84 (www.google.com)	272 B / 164 B

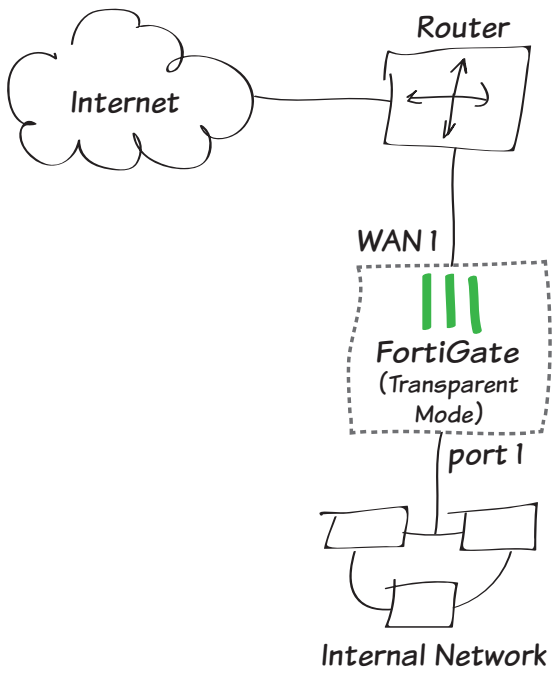
Watch the video

Installing a FortiGate in Transparent mode

In this example, you will learn how to connect and configure a new FortiGate unit in Transparent mode to securely connect a private network to the Internet. In Transparent mode, the FortiGate applies security scanning to traffic without applying routing or network address translation (NAT).

Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the **System Information** widget, found at **System > Dashboard > Status**.

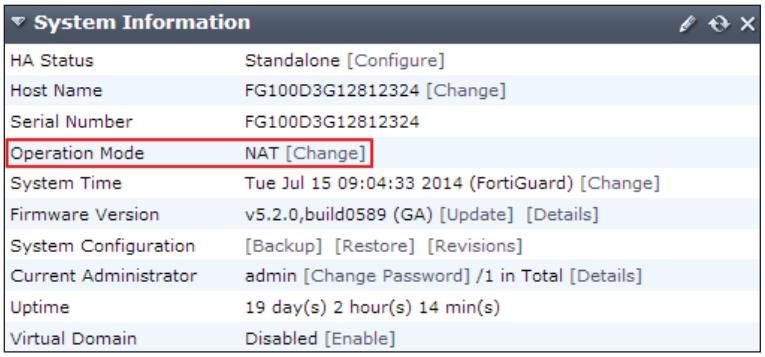
1. Changing the FortiGate's operation mode
2. (Optional) Setting the FortiGate's DNS servers
3. Creating a policy to allow traffic from the internal network to the Internet
4. Connecting the network devices



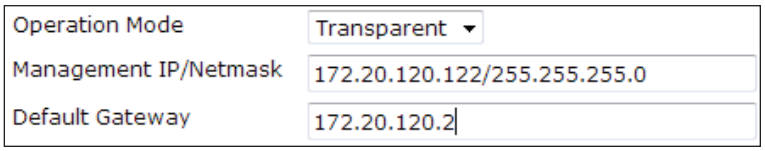
1. Changing the FortiGate's operation mode

Go to **System > Dashboard > Status** and locate the **System Information** widget.

Beside **Operation Mode**, select **Change**.



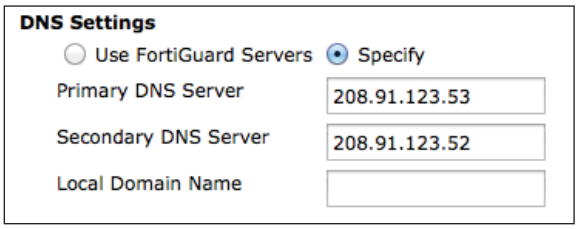
Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network.



You can now access the GUI by browsing to the Management IP address (in the example, you would browse to *http://172.20.120.122*).

2. (Optional) Setting the FortiGate's DNS servers

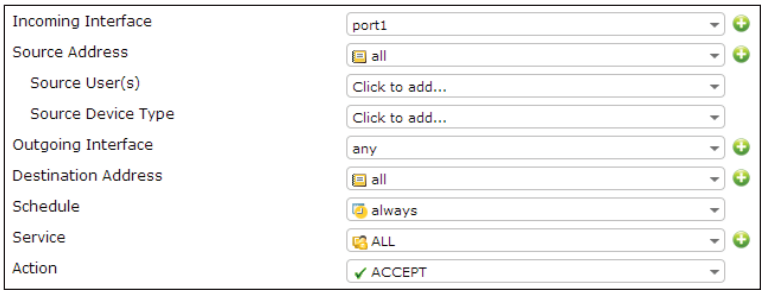
The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.



3. Creating a policy to allow traffic from the internal network to the Internet

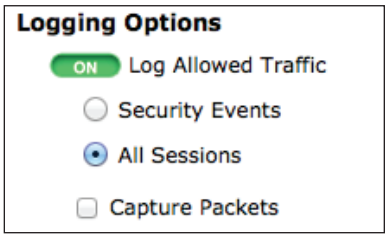
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to an available external interface (typically port 1) and the **Outgoing Interface** to the Internet-facing interface (typically WAN1).



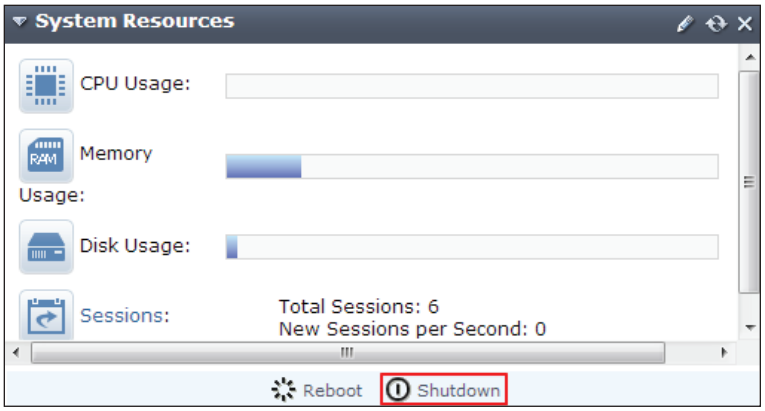
It is recommended to avoid using any security profiles until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



4. Connecting the network devices

Go to **System > Dashboard > Status** and locate the **System Resources** widget. Select **Shutdown** to power off the FortiGate unit.



Alternatively, you can enter the following command in the **CLI Console** (also found by going to **System > Dashboard > Status**):

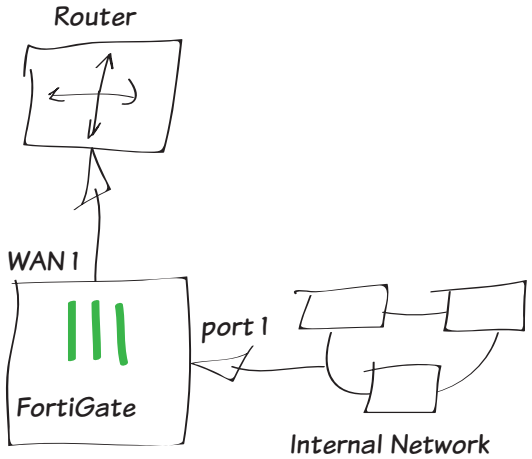
```
execute shutdown
```

Wait until all the lights, except for the power light, on your FortiGate have turned off. If your FortiGate has a power button, use it to turn the unit off. Otherwise, unplug the unit.

You can now connect the FortiGate unit between the internal network and the router.

Connect the wan1 interface to the router internal interface and connect the internal network to the FortiGate internal interface port.

Power on the FortiGate unit.



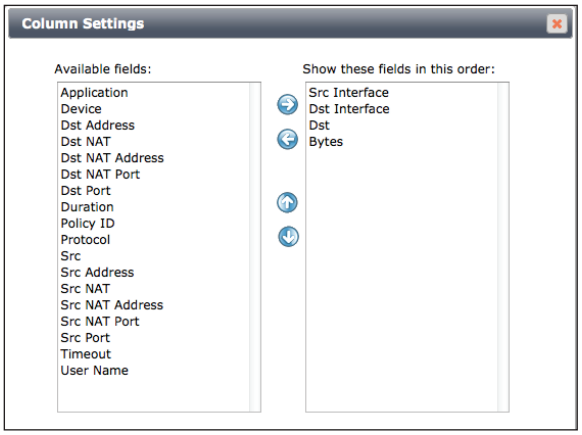
5. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has port 1 as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

#	Src Interface	Dst Interface	Dst	Bytes (Sent/Received)
1	wan1	wan1	172.20.120.122	6,567
2	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	236
3	port1	wan1	s.yimg.com (68.142.250.160:443)	1,026,162
4	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	262
5	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	291
6	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	178
7	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204
8	port1	wan1	safebrowsing-cache.google.com (184.150.152.152:443)	10,721
9	port1	wan1	BN1WNS1011410.wns.windows.com (157.56.98.65:443)	7,903
10	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	211
11	port1	wan1	google-public-dns-a.google.com (8.8.8.8:53)	385
12	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	226
13	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	173
14	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	413
15	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204
16	port1	wan1	safebrowsing-cache.google.com (184.150.152.178:443)	876,026
17	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	184
18	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	441
19	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	212
20	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204

If these two columns are not shown, select **Column Settings** and move **Src Interface** and **Dst Interface** to the list of fields to be shown.



Watch the video

Troubleshooting your installation

If your FortiGate does not function as desired after completing the installation, try the following troubleshooting methods. Most methods can be used for FortiGates in both NAT/Route and Transparent mode. Any exceptions are marked.

1. Use FortiExplorer if you can't connect to the FortiGate over Ethernet.

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.

2. Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate unit LED indicators.

3. Check the physical network connections.

Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged. Make sure that each cable connects to the correct device and the correct Ethernet port on that device. Also, check the **Unit Operation** widget, found at **System > Dashboard > Status**, to make sure the connected interfaces are shown in green.

4. Verify that you can connect to the internal IP address of the FortiGate unit (NAT/Route mode).

Connect to the web-based manager from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.

If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the web-based manager, check the settings for administrative access on that interface.

5. Verify that you can connect to the management IP address of the FortiGate unit (Transparent mode).

From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

6. Check the FortiGate interface configurations (NAT/Route mode).

Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure Addressing Mode is set to the correct mode.

7. Verify the security policy configuration.

Go to **Policy & Objects > Policy > IPv4** (or **Policy & Objects > Policy > IPv6**) and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the **Sessions** column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select **Sessions**, and select **Apply**).

If you are using NAT/Route mode, check the configuration of the policy to make sure that **NAT** is turned on and that **Use Destination Interface Address** is selected.

8. Verify that you can connect to the Internet-facing interface's IP address (NAT/Route mode).

Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate unit is not allowing sessions from the internal interface to the Internet-facing interface.

9. Verify the static routing configuration (NAT/Route mode).

Go to **Router > Static > Static Routes** (or **System > Network > Routing**) and verify that the default route is correct. View the **Routing Monitor** (found either on the same page or at **Router > Monitor > Routing Monitor**) and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as **Connected**, one for each connected FortiGate interface.

10. Verify that you can connect to the gateway provided by your ISP.

Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.

11. Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

12. Verify the DNS configurations of the FortiGate unit and the PCs.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`. If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

13. Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, confirm that it can reach FortiGuard.

First, check the License Information widget to make sure that the status of all FortiGuard services matches the services that you have purchased. Go to **System > Config > FortiGuard**. Expand **Web Filtering and Email Filtering Options** and select **Test Availability**. After a minute, the GUI should show a successful connection.

14. Consider changing the MAC address of your external interface (NAT/Route mode).

Some ISPs do not want the MAC address of the device connecting to their network cable to change and so you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
   edit <interface>
      set macaddr <xx:xx:xx:xx:xx:xx>
   end
end
```

15. Check the FortiGate bridge table (Transparent mode).

When the FortiGate is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit. Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues and there are no bridges listed, that is a likely cause. Check for the MAC address of the interface or device in question.

To list the existing bridge instances on the FortiGate unit, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. Check the device's network connections and make sure they are connected and operational

16. Either reset the FortiGate unit to factory defaults or contact the technical assistance center.

If all else fails, reset the FortiGate unit to factory defaults using the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.

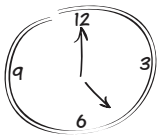
You can also contact the technical assistance center. For contact information, go to support.fortinet.com.

FortiGate registration and basic settings

In this example, you will register your FortiGate unit and set the system time. You will also configure several administrative account settings to prevent unauthorized access.

1. Registering your FortiGate
2. Setting the system time
3. (Optional) Restricting administrative access to a trusted host
4. Changing the default admin password
5. Results

Register your FortiGate



Set the system time

Configure the admin account

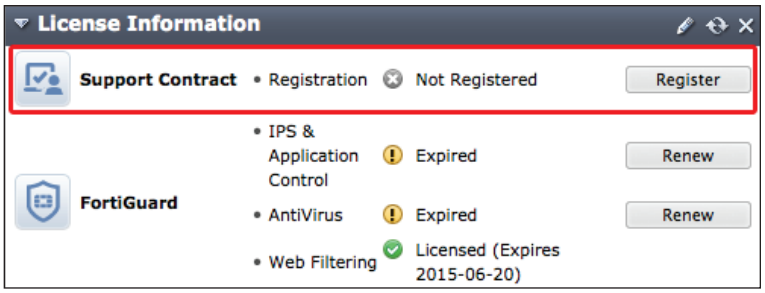
1. Registering your FortiGate

Registering your FortiGate allows you to receive FortiGuard updates and is required for firmware upgrades and access to support.fortinet.com.

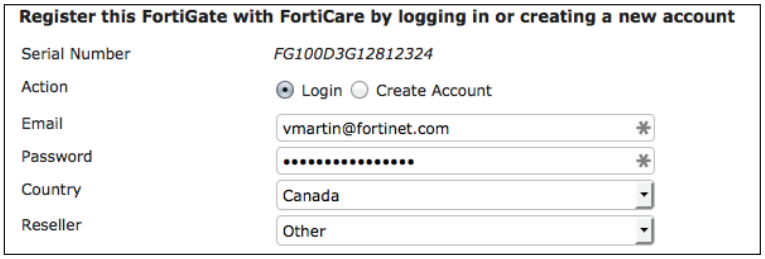
Before registering your FortiGate unit, it must have Internet connectivity.

Go to **System > Dashboard > Status** and locate the **License Information** widget.

Next to **Support Contract**, select **Register**.

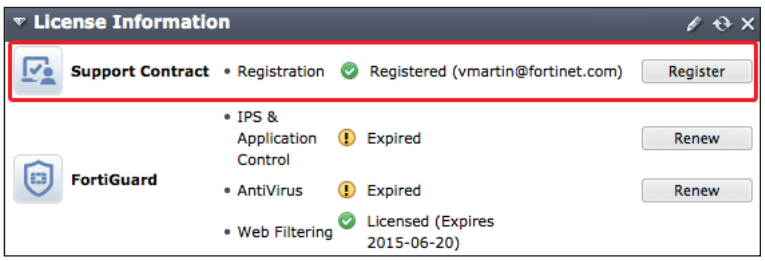


Either use an existing Fortinet Support account or create a new one. Select your **Country** and **Reseller**.



It is recommend to use a common account to register all your Fortinet products, to allow the Support site to keep a complete listing of your devices.

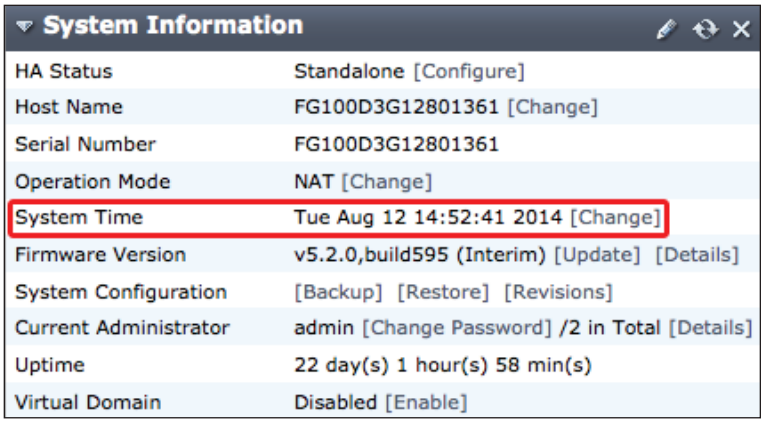
The **License Information** widget now displays the unit as **Registered**.



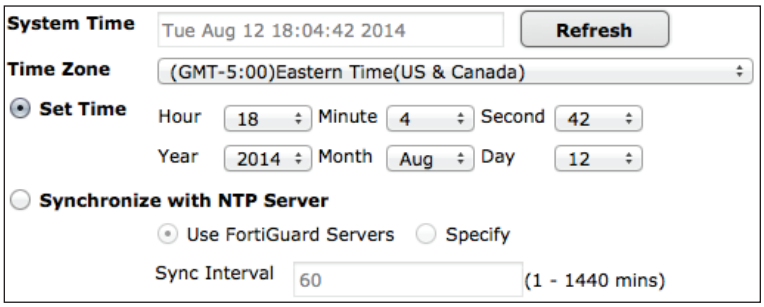
2. Setting the system time

Go to **System > Dashboard > Status** and locate the **System Information** widget.

Next to **System Time**, select **Change**.

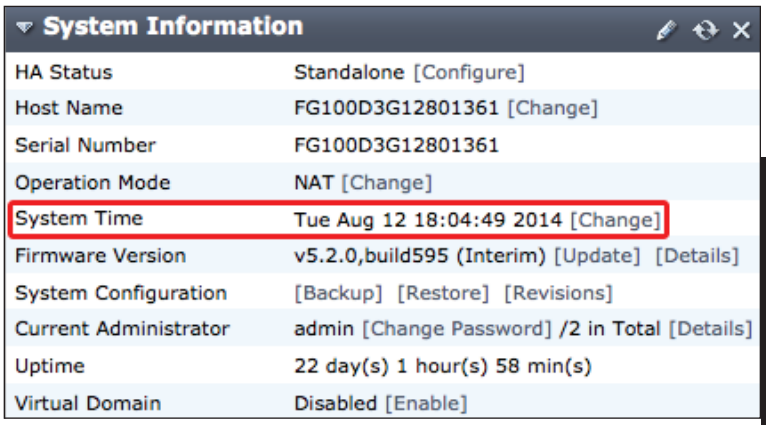


Select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.



Since not all time zones have names, you may need to know how many hours ahead (+) or behind (-) you are from Greenwich Mean Time (GMT).

The **System Information** widget now displays the correct time.



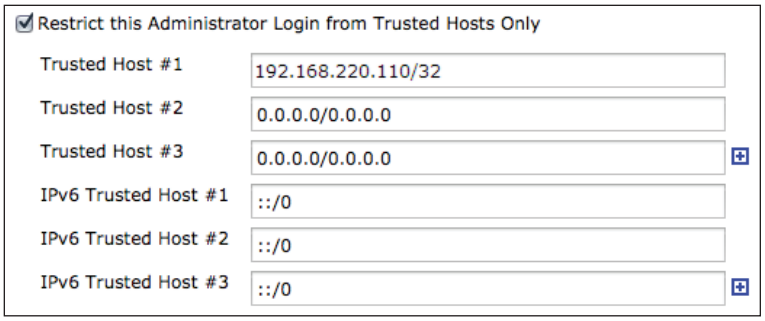
3. (Optional) Restricting administrative access to a trusted host

Go to **System > Admin > Administrators** and edit the default *admin* account.

Enable **Restrict this Administrator Login from Trusted Hosts Only**. Set **Trusted Host #1** to the static IP address of the PC you will use to administer the FortiGate unit, using /32 as the netmask.

You can also set an entire subnet as the trusted host, using /24 as the netmask.

If required, set additional trusted hosts.

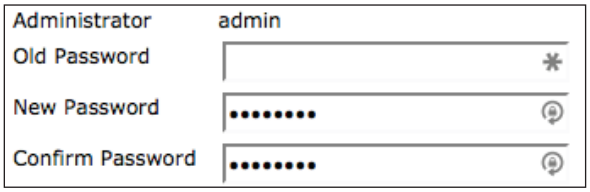


4. Changing the default admin password

Go to **System > Admin > Administrators** and edit the default *admin* account.

Select **Change Password**. Leave **Old Password** blank and enter the **New Password**.

You will be automatically signed out after changing the password.

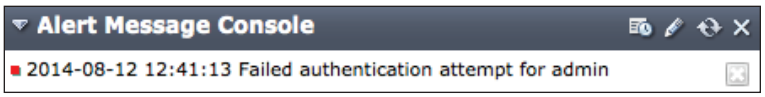


5. Results

Attempt to log in using the *admin* account without a password. Access is denied.

Log in using the admin account with your new password. Access is granted.

Go to **System > Dashboard > Status** and locate the **Alert Message Console** widget, which indicates the failed authentication attempt.



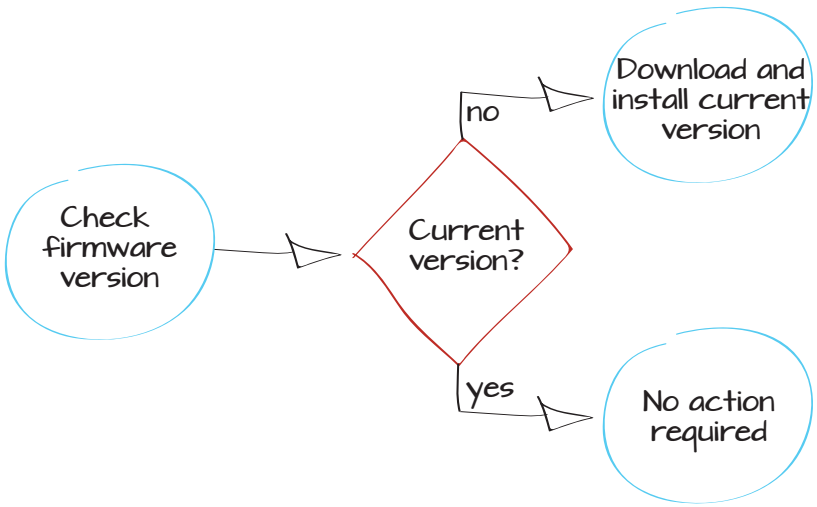
(Optional) If access has been restricted to a trusted host, attempts to connect from a device that is not trusted will be denied.

Updating the FortiGate's firmware

This example verifies the current version of FortiOS firmware and, if necessary, updates it to the latest version. FortiOS is the operating system used by FortiGate and FortiWiFi units. Updating FortiOS ensures the FortiGate unit makes use of the latest tools and security features available.

Always review the Release Notes and Supported Upgrade Paths documentation before installing a new firmware. These documents can be found at http://docs.fortinet.com.

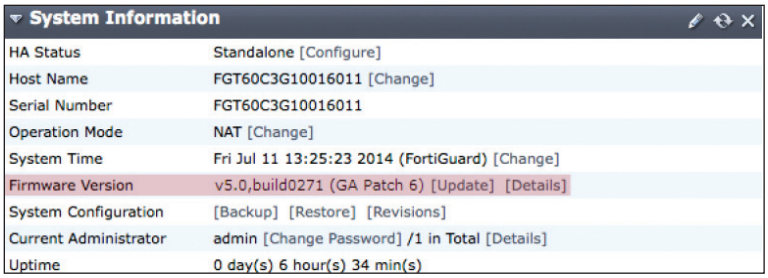
1. Checking the current FortiOS firmware
2. Downloading the latest FortiOS firmware
3. Updating the FortiGate to the latest firmware
4. Results



1. Checking the current FortiOS firmware

Log in to the web-based manager and go to **System > Dashboard > Status** and view the **System Information** dashboard widget to see the **Firmware Version** currently installed on your FortiGate unit.

Go to http://docs.fortinet.com/fortigate/release-information and refer to the Release Information section to determine the most recent version of FortiOS.

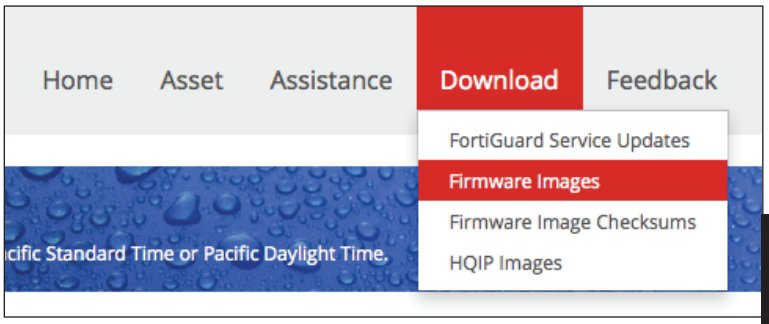


2. Downloading the latest FortiOS firmware

To download a new firmware version, browse to https://support.fortinet.com and log in using your Fortinet account ID/email and password.

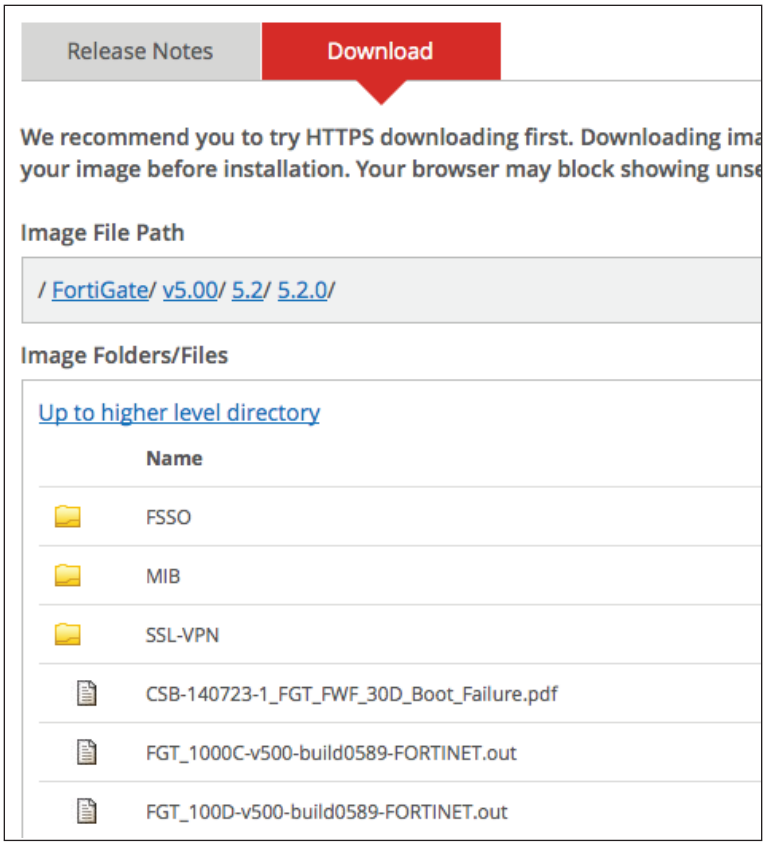
Your FortiGate unit must be registered before you can access firmware images from the Support site.

Go to **Download > Firmware Images**.



From the **Select Product** dropdown menu, choose **FortiGate**.

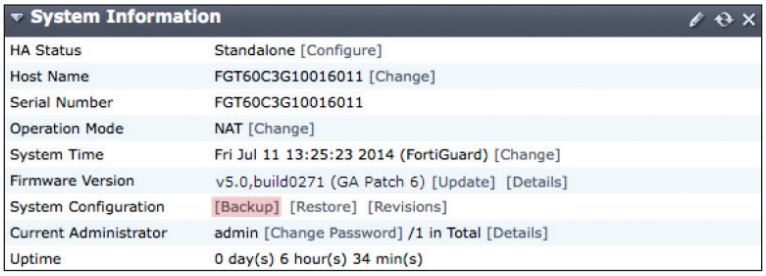
Locate and download the firmware for your FortiGate model.



3. Updating the FortiGate to the latest firmware

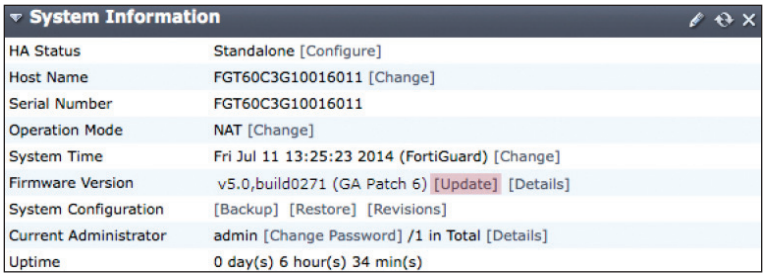
Go to **System > Dashboard > Status**.

Backup your configuration from the **System Information** dashboard widget, next to **System Configuration**. Always remember to back up your configuration before doing any firmware upgrades.



Under **System Information > Firmware Version**, select **Update**.

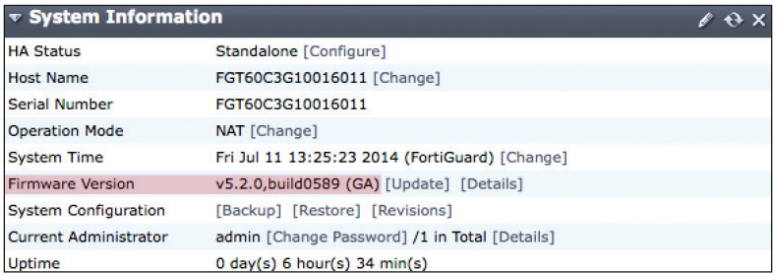
Find the firmware image file that you downloaded and select **OK** to upload and install the firmware build on the FortiGate unit.



4. Results

The FortiGate unit uploads the firmware image file, updates to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

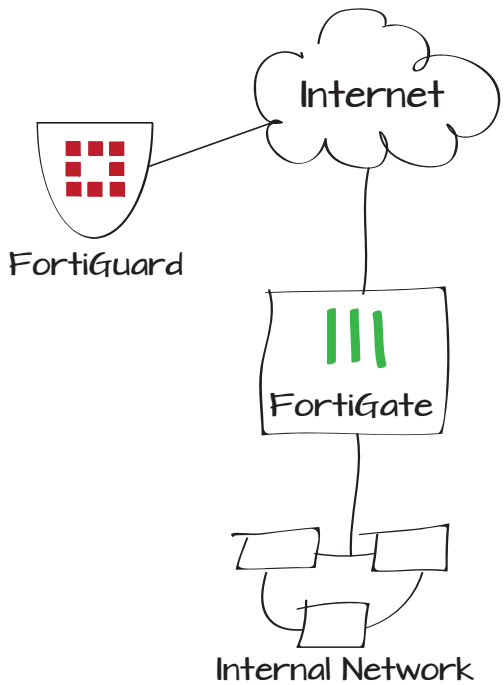
From the FortiGate web-based manager, go to **System > Dashboard > Status**. In the **System Information** dashboard widget, the **Firmware Version** will show the updated version of FortiOS.



Setting up FortiGuard services

If you have purchased FortiGuard services and registered your FortiGate unit, the FortiGate should automatically connect to FortiGuard and display license information about your FortiGuard services. In this example, you will verify whether the FortiGate unit is communicating with the FortiGuard Distribution Network (FDN) by checking the License Information dashboard widget.

1. Verifying the connection
2. Troubleshooting communication errors
3. Results



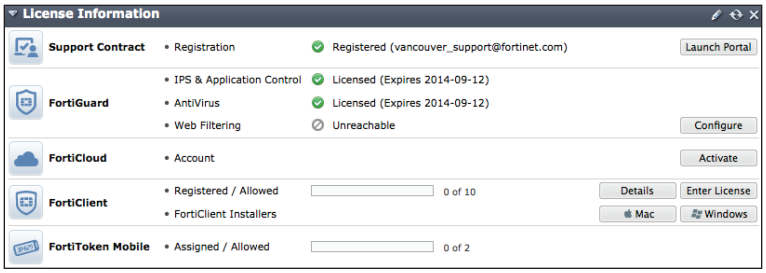
1. Verifying the connection

Go to **System > Dashboard > Status** and go to the **License Information** widget.

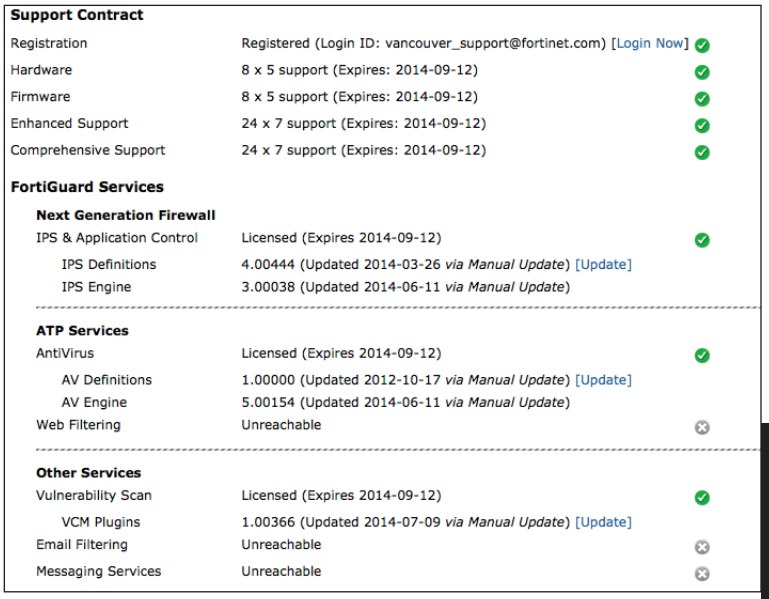
Any subscribed services should have a , indicating that connections are successful.

A indicates that the FortiGate unit cannot connect to the FortiGuard network, or that the FortiGate unit is not registered.

A indicates that the FortiGate unit was able to connect but that a subscription has expired or has not been activated.



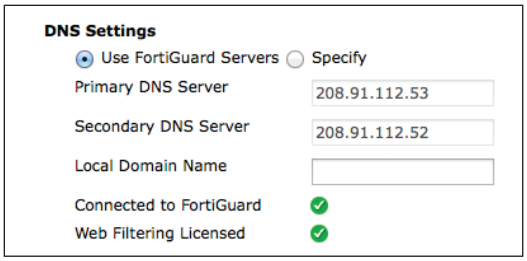
You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.



2. Troubleshooting communication errors

Go to **System > Network > DNS** and ensure that the primary and secondary DNS servers are correct.

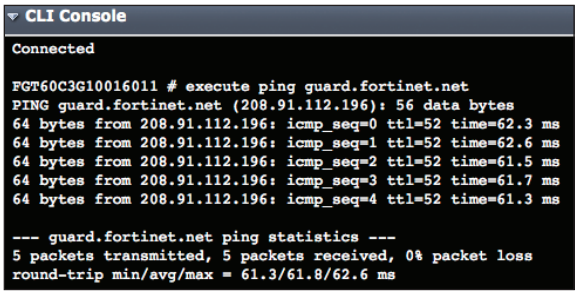
In this screenshot the FortiGate has been successfully tested already.



To test if you are connected to the correct DNS server go to **System > Dashboard > Status** and enter the following command into the **CLI Console**:

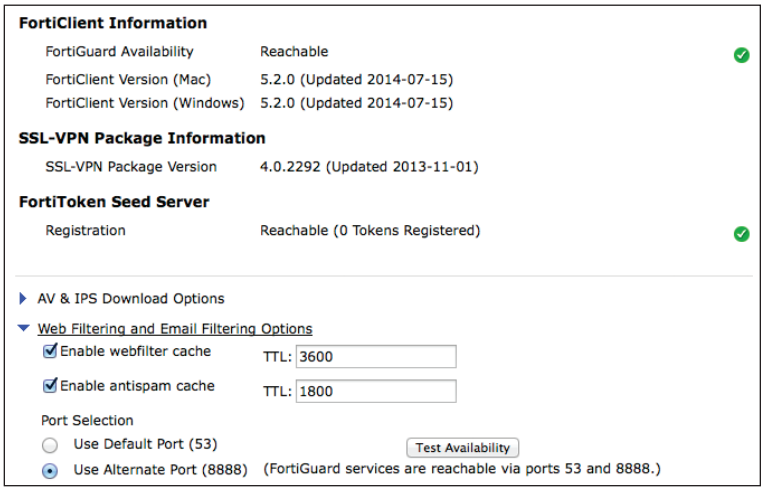
```
execute ping guard.fortinet.net
```

If the connection is successful, the **CLI Console** should display a similar output as the example.



To test if the FortiGuard services are reachable, go to **System > Config > FortiGuard**. Under the **Web Filtering and Email Filtering Options** click **Test Availability**. This will indicate which ports are open.

If the FortiGate default port (53) cannot be unblocked, go to **System > Config > FortiGuard**. Under the **Web Filtering and Email Filtering Options** choose **Use Alternate Port (8888)**.

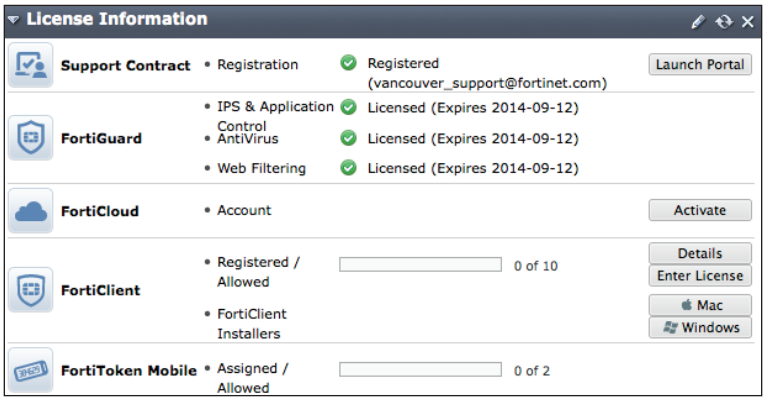


If you are updating using the FortiManager, the FortiGate unit can also use port 80. If further problems occur, you may have to unblock ports using the CLI. See page 480 of the CLI Reference for FortiOS 5.2. for more information.

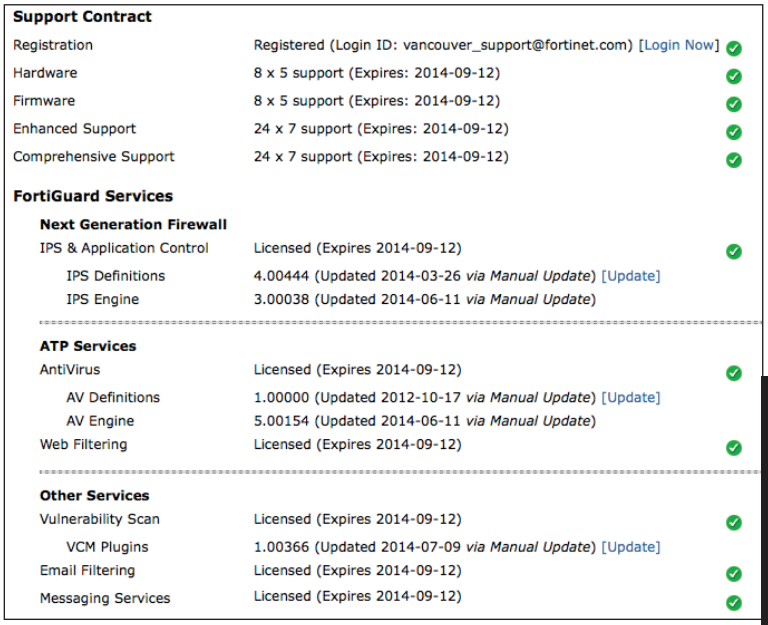
3. Results

Go to **System > Dashboard > Status** and go to the **License Information** widget.

Any subscribed services should have a , indicating that connections have been established and that the licenses have been verified.



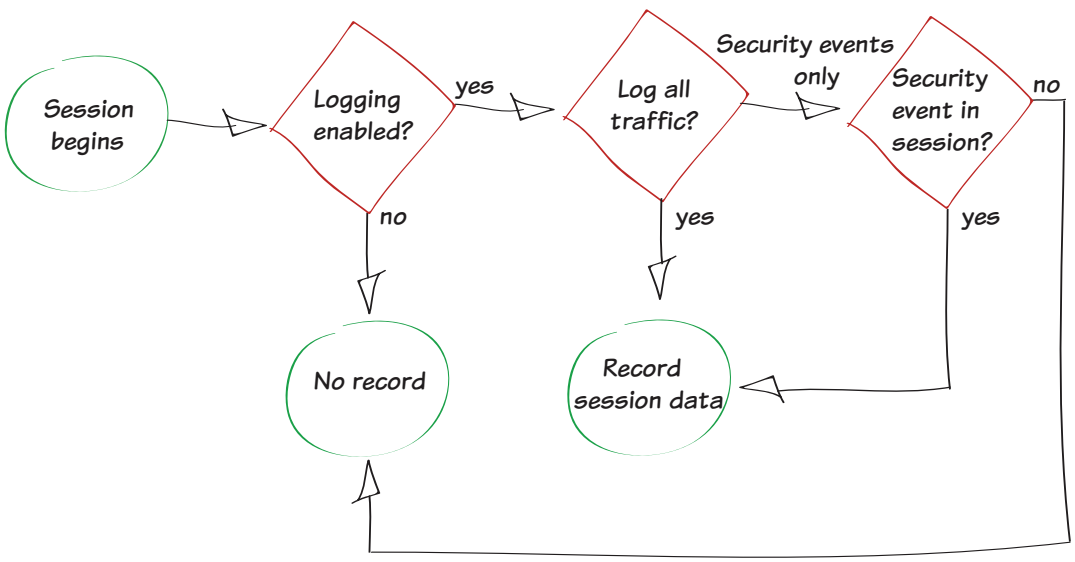
Go to **System > Config > FortiGuard**. Features and services you are subscribed to should have a , indicating that connections are successful.



Logging FortiGate traffic

This example demonstrates how to enable logging to capture the details of the network traffic processed by your FortiGate unit. Capturing log details will provide you with detailed traffic information that you can use to asses any network issues.

1. Recording log messages and enabling event logging
2. Enabling logging in the security policies
3. Results



1. Recording log messages and enabling event logging

Go to **Log & Report > Log Config > Log Settings**.

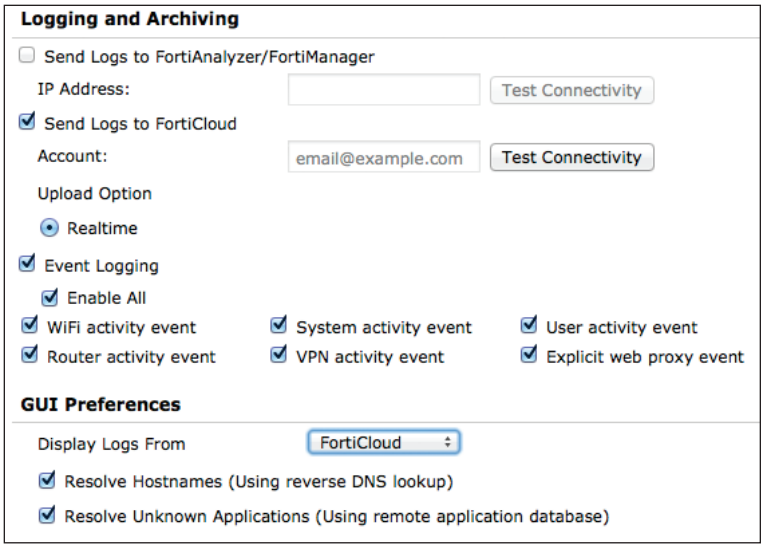
Select where log messages will be recorded. You can save log messages to disk if it is supported by your FortiGate unit, to a FortiAnalyzer or FortiManager unit if you have one, or to FortiCloud if you have a subscription. Each of these options allow you to record and view log messages and to create reports based on them.

In most cases, it is recommended to **Send Logs to FortiCloud**, as shown in the example.

Next, enable **Event Logging**.

You can choose to **Enable All** types of logging, or specific types, such as **WiFi activity events**, depending on your needs.

Under the **GUI Preferences** ensure that the **Display Logs From** is set to the same location where the log messages are recorded (in the example **FortiCloud**).

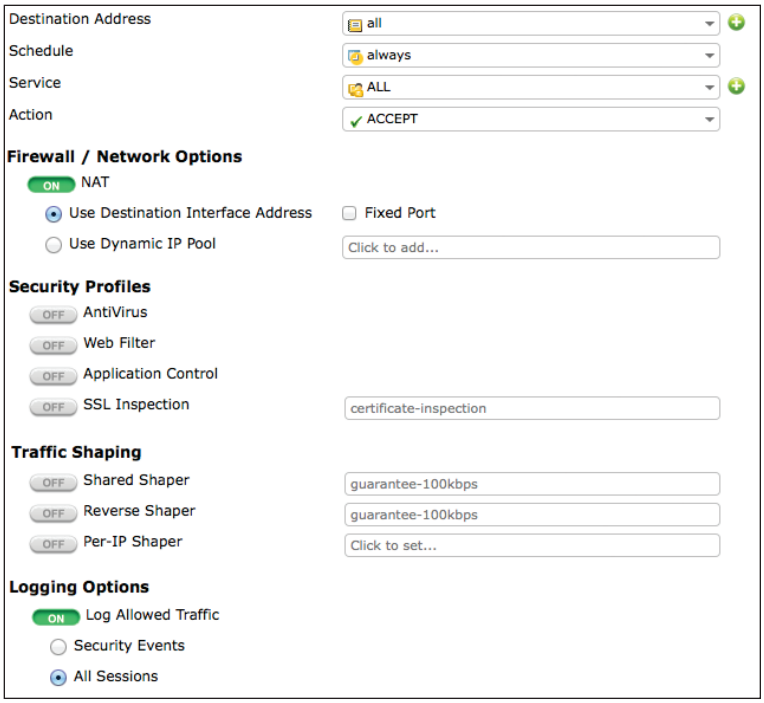


2. Enabling logging in the security policies

Go to **Policy & Objects > Policy > IPV4**. Edit the policies controlling the traffic you wish to log.

Under **Logging Options**, select either **Security Events** or **All Sessions**.

In most cases, you should select Security Events. All Sessions provides detailed traffic analysis but also but requires more system resources and storage space.



3. Results

View traffic logs by going to **Log & Report > Traffic Log > Forward Traffic**. The logs display a variety of information about your traffic, including date/time, source, device, and destination.

To change the information shown, right-click on any column title and select **Column Settings** to enable or disable different columns.

Date/Time	Src	Device	Dst
10:23:02	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70
10:22:23	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.53
10:22:02	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:20:03	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53
10:18:58	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.50
10:18:51	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:15:43	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:13:44	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53
10:12:54	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70
10:12:32	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184

Creating security policies

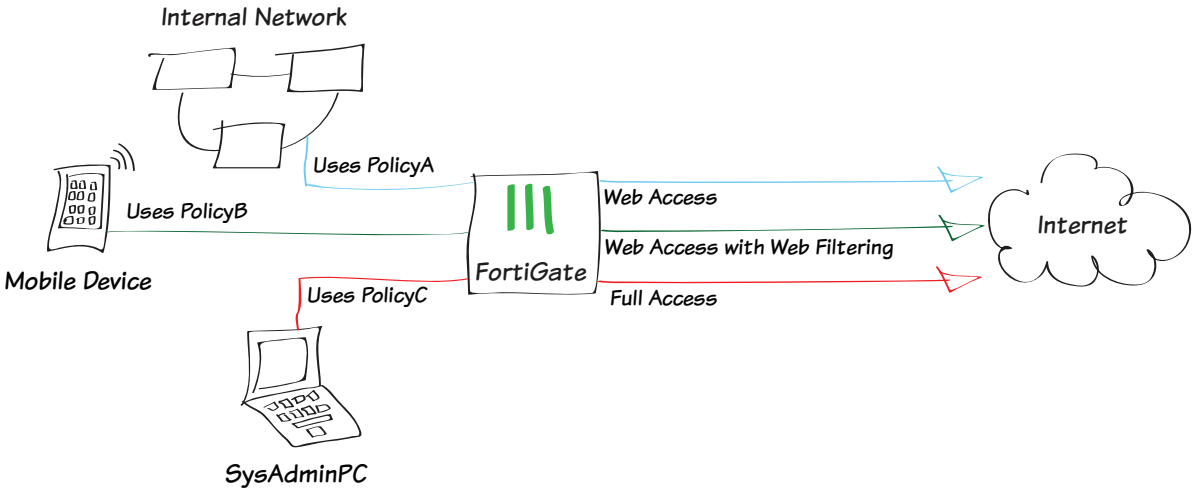
This example shows how to create and order multiple security policies in the policy table, in order to apply the appropriate policy to various types of network traffic.

In the example, three IPv4 policies will be configured. PolicyA will be a general policy allowing Internet access to the LAN. PolicyB will allow Internet access while applying web filtering for specific mobile devices connecting through the LAN. PolicyC will allow the system administrator's PC (named SysAdminPC) to have full access.

A fourth policy, the default "deny" policy, will also be used.

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN.

1. Configuring PolicyA to allow general web access
2. Creating PolicyB to allow access for mobile devices
3. Defining SysAdminPC
4. Creating PolicyC to allow access for SysAdminPC
5. Ordering the policy table
6. Results

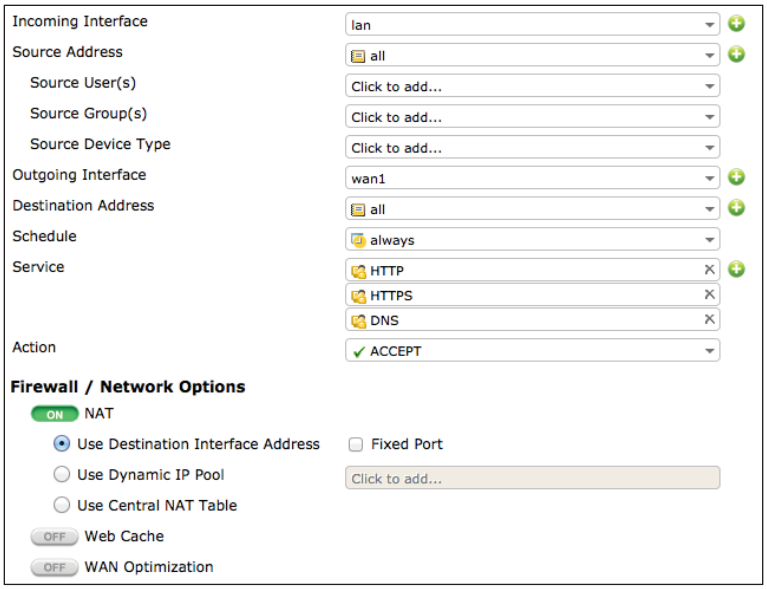


1. Configuring PolicyA to allow general web access

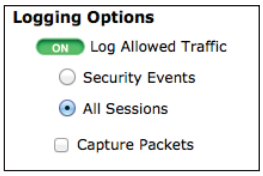
Go to **Policy & Objects > Policy > IPv4** and edit the policy allowing outgoing traffic.

Set **Service** to **HTTP**, **HTTPS**, and **DNS**.

Ensure that you have enabled **NAT**.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



2. Creating PolicyB to allow access for mobile devices

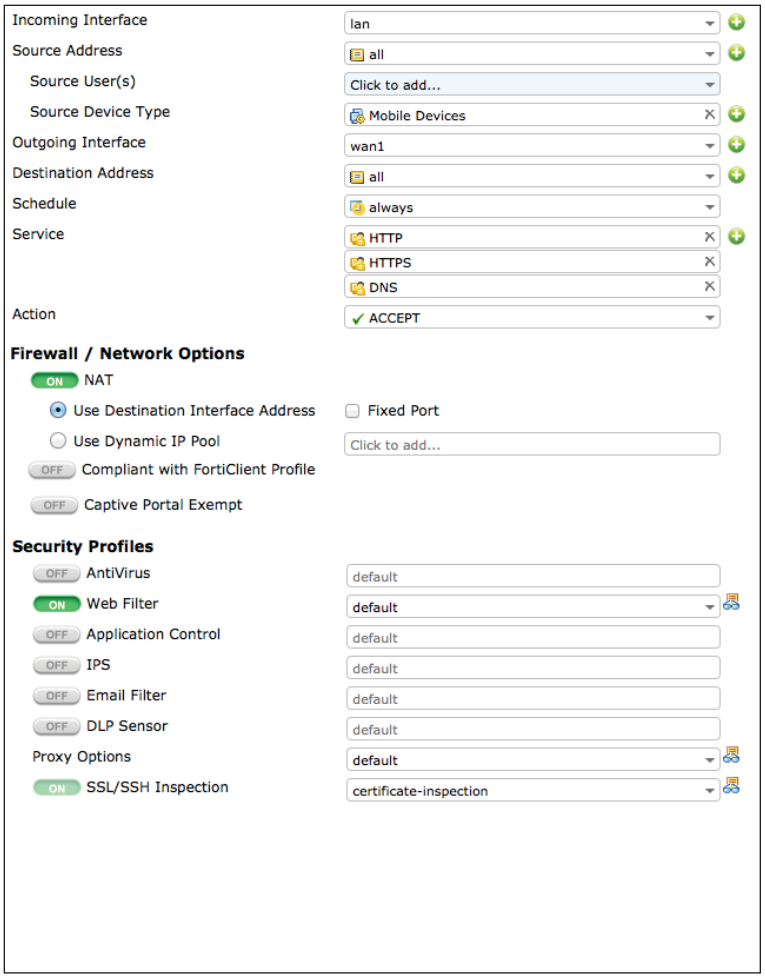
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to **lan**, **Source Device Type** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and **Service** to **HTTP**, **HTTPS**, and **DNS**.

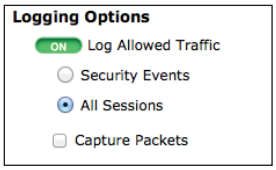
Enable **NAT**.

Under **Security Profiles**, enable **Web Filter** and set it to use the **default** profile. This action will enable **Proxy Options** and **SSL Inspection**. Use the **default** profile for Proxy Options and set SSL Inspection to **certificate-inspection** to allow HTTPS traffic to be inspected.

Using a device group will automatically enable device identification on the **lan** interface.



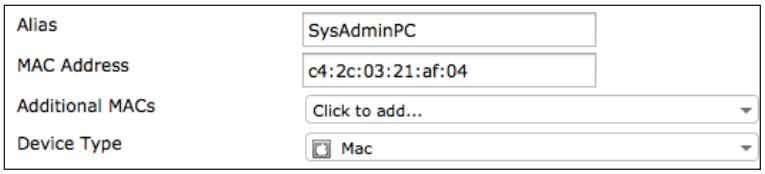
Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



3. Defining SysAdminPC

Go to **User & Device > Device > Device Definitions** and create a new definition for the system administrator's PC.

Select an approprate **Alias**, then set the **MAC Address**. Set the appropriate **Device Type**.

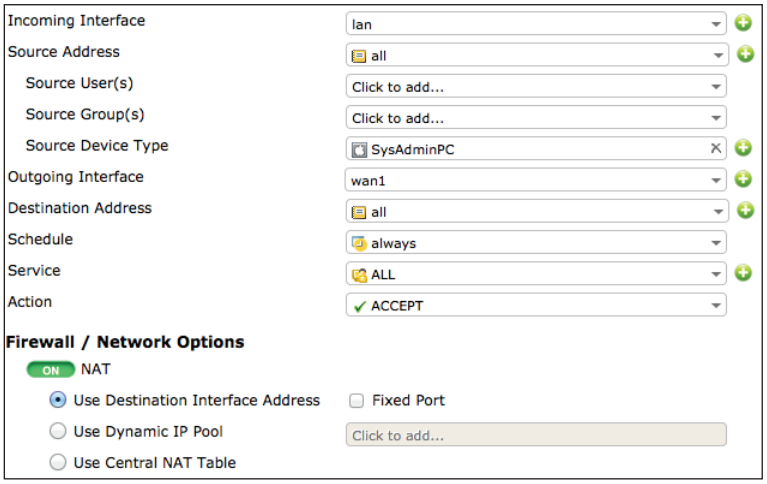


4. Configuring PolicyC to allow access for SysAdminPC

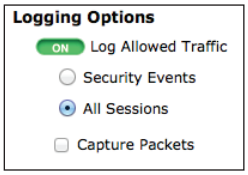
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to **lan**, **Source Device Type** to SysAdminPC, **Outgoing Interface** to your Internet-facing interface, and **Service** to **ALL**.

Enable **NAT**.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



5. Ordering the policy table

Go to **Policy & Objects > Policy > IPv4** to view the policy table.

Currently, the policies are arranged in the order they were created: PolicyA is at the top, followed by PolicyB, PolicyC, and the default deny policy. In order to have the correct traffic flowing through each policy, they must be arranged so that the more specific policies are located at the top.

Seq.#	From	To	Service	Web Filter	Devices
1	lan	wan1	HTTP HTTPS DNS		
2	lan	wan1	HTTP HTTPS DNS	WEB default	Mobile Devices
3	lan	wan1	ALL		SysAdminPC
4	any	any	ALL		

In the example, the policy table has been set to show only the columns that best display the differences between the policies. To do this, right-click on the top of the table, select or deselect columns as necessary, then select **Apply**.

To reorder the policies, select any area in the far-left column (in the example, **Seq.#**) for PolicyB and drag the policy to the top of the list. Repeat this for PolicyC, so that the order is now PolicyC, PolicyB, PolicyA, and the default deny policy.

Refresh the page to see the updated **Seq.#** values.

Seq.#	From	To	Service	Web Filter	Devices
1	lan	wan1	ALL		SysAdminPC
2	lan	wan1	HTTP HTTPS DNS	WEB default	Mobile Devices
3	lan	wan1	HTTP HTTPS DNS		
4	any	any	ALL		

6. Results

Browse the Internet using the system administrator's PC, a different PC, and a mobile device.

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic from the three devices flows through different policies. In the example, the SysAdmin PC (IP 10.10.11.10), a Windows PC (IP 10.10.11.14), and an iPad (IP 10.10.11.13) were used to generate traffic.

#	Policy ID	Date/Ti...	Source	Destination	Device
1	3	13:42:18	10.10.11.10	72.167.239.239 (ocsp.godaddy.com.akadns.net)	SysAdminPC
2	3	13:42:18	10.10.11.10	208.91.114.193	SysAdminPC
3	3	13:42:18	10.10.11.10	192.0.65.242 (polldaddy.com)	SysAdminPC
4	3	13:42:18	10.10.11.10	208.91.114.193	SysAdminPC
5	3	13:42:18	10.10.11.10	192.0.65.242 (polldaddy.com)	SysAdminPC
6	3	13:42:18	10.10.11.10	208.91.114.193	SysAdminPC
7	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
8	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
9	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
10	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
11	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
12	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
13	2	13:39:51	10.10.11.13	17.134.126.129 (gs-loc.ls-apple.com.akadns.net)	d8:a2:5e:1d:b1:a6
14	2	13:39:34	10.10.11.13	66.235.138.194 (metrics.apple.com)	d8:a2:5e:1d:b1:a6
15	2	13:39:34	10.10.11.13	184.87.13.15 (e3191.dscc.akamaiedge.net)	d8:a2:5e:1d:b1:a6
16	2	13:39:34	10.10.11.13	23.0.160.208 (images.apple.com)	d8:a2:5e:1d:b1:a6

Policy ID is automatically assigned to a policy when it is created, and so, in the example, the ID for PolicyA is 1, PolicyB is 2, and PolicyC is 3.

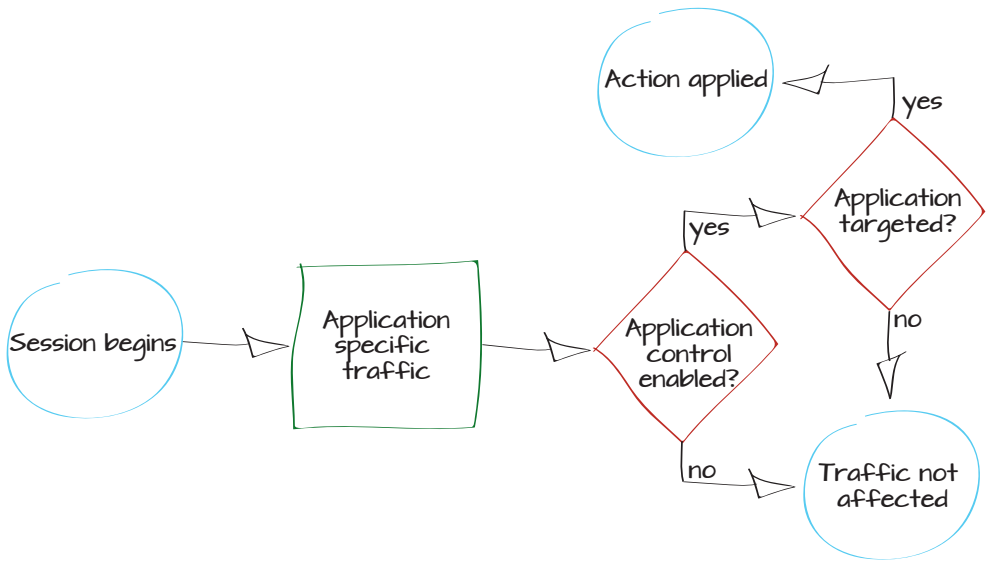
(Optional) Attempt to make an SSL connection to a web server with all three devices. Only the system administrator's PC will be able to connect.

Watch the video

Blocking P2P traffic and YouTube applications

In this example, you will learn how to use Application Control to monitor traffic and determine if there are any applications currently in use that should not have network access. If you discover any applications that you wish to block, application control will then be used to ensure that these applications cannot access the network.

1. Enabling Application Control and multiple security profiles
2. Using the default application profile to monitor network traffic
3. Adding the default profile to a security policy
4. Reviewing the FortiView dashboards
5. Creating an application profile to block applications
6. Adding the blocking sensor to a security policy
7. Results



1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.

Select **Show More** and enable **Multiple Security Profiles.**

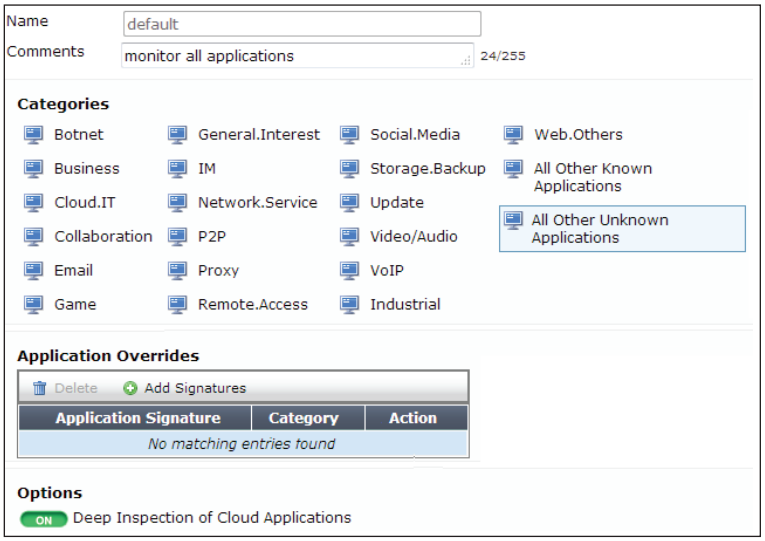
Apply the changes.

2. Using the default application profile to monitor network traffic

Go to **Security Profiles > Application Control** and view the **default** profile.

A list of application **Categories** is shown. By default, most categories are already set to **Monitor**. In order to monitor all applications, select **All Other Known Applications** and set it to Monitor. Do the same for **All Other Unknown Applications**.

The default profile also has **Deep Inspection of Cloud Applications** turned **ON**. This allows web-based applications, such as video streaming, to be monitored by your FortiGate.



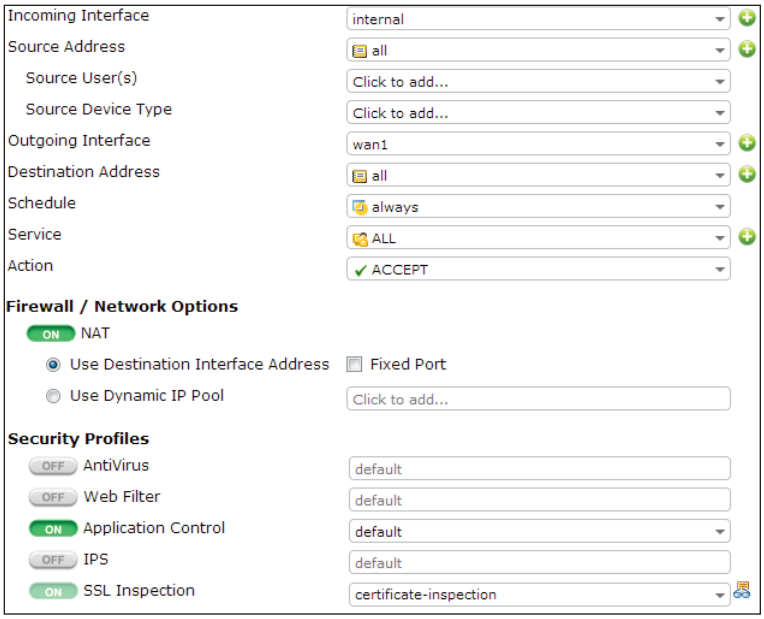
3. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows outgoing traffic from your network.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see "Preventing certificate errors" on page 49.

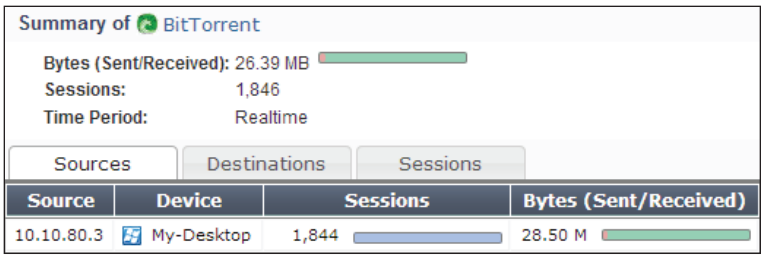


4. Reviewing the FortiView dashboards

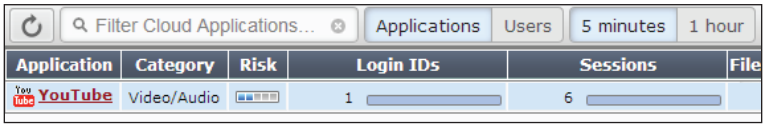
Go to **System > FortiView > Applications** and select the **now** view.

This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).

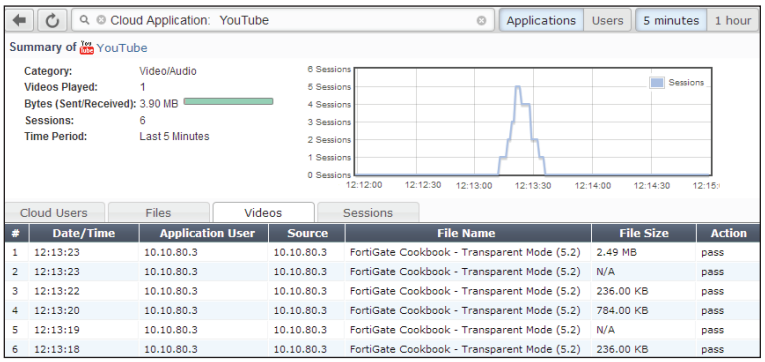
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.



Similar information can be viewed for Cloud Applications by going to **System > FortiView > Cloud Applications** and selecting **Applications** that have been used in the last **5 Minutes**.



Cloud Applications also have drilldown options, including the ability to see which videos have been viewed if streaming video traffic was detected.



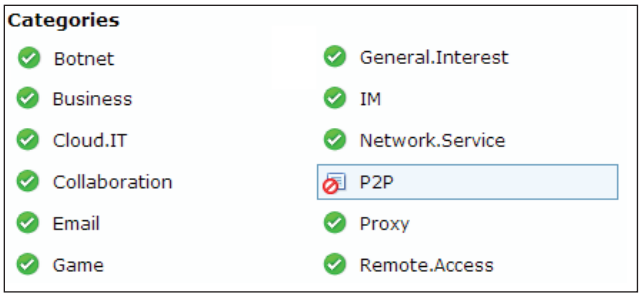
5. Creating an application profile to block applications

In the above example, traffic from BitTorrent, a Peer-to-Peer (P2P) downloading application, was detected. Next, you will create an application control profile that will block P2P traffic.

The new profile will also block all applications associated with Youtube, without blocking other applications in the **Video/Audio** category.

Go to **Security Profiles > Application Control** and create a new profile.

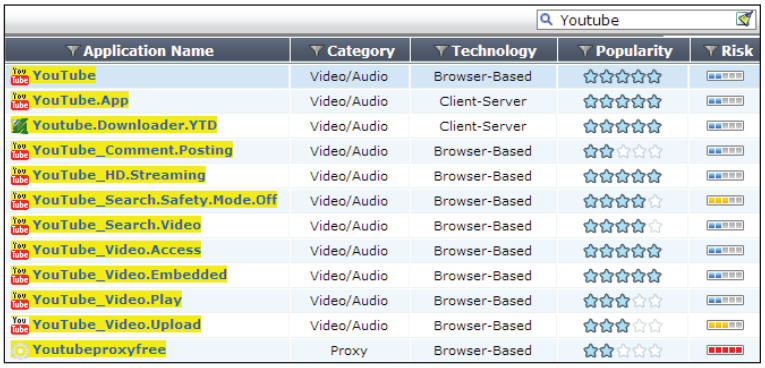
Select the **P2P** category and set it to **Block**.



Under **Application Overrides**, select **Add Signatures**.

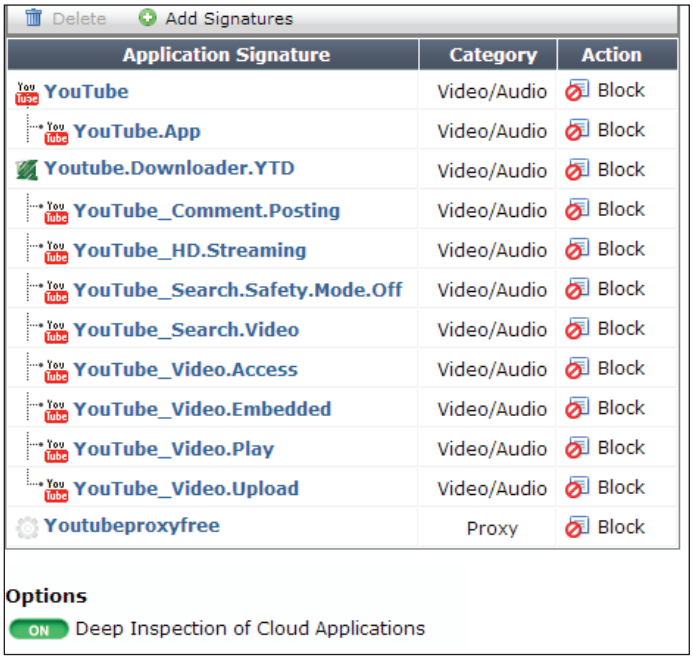
Search for *Youtube* and select all the signatures that are shown.

Select **Use Selected Signatures**.



The signatures have been added to the Application Overrides list and have automatically been set to Block.

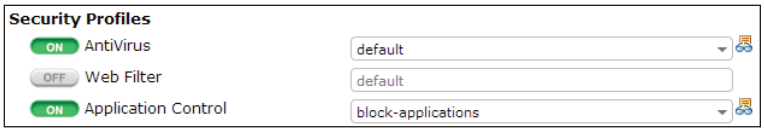
Enable **Deep Inspection of Cloud Applications.**



6. Adding the blocking sensor to a security policy

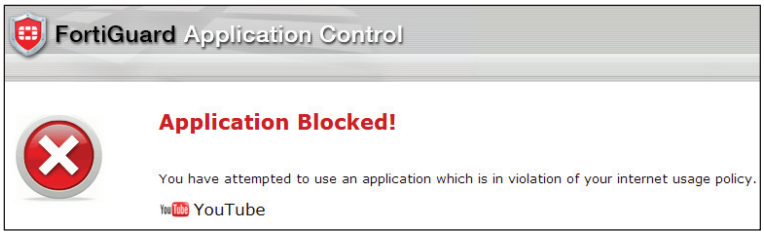
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows outgoing traffic from your network.

Set **Application Control** to use the new profile.



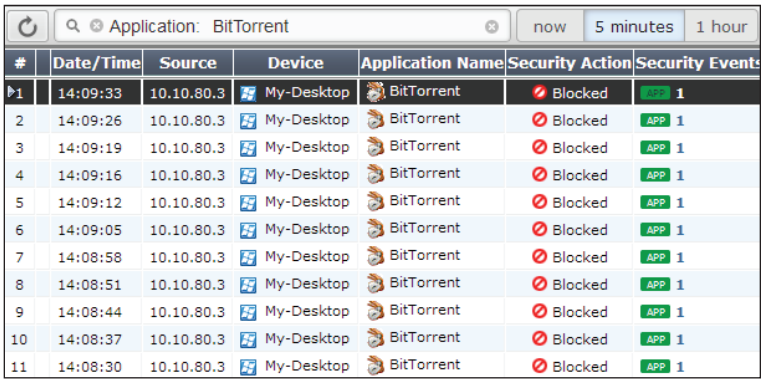
7. Results

Attempt to browse to www.youtube.com. A warning message will appear, stating that the application was blocked.



Traffic from BitTorrent applications will also be blocked.

To see information about this blocked traffic, go to **System > FortiView > All Sessions**, select the **5 minutes** view, and filter the traffic by application.



#	Date/Time	Source	Device	Application Name	Security Action	Security Events
1	14:09:33	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
2	14:09:26	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
3	14:09:19	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
4	14:09:16	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
5	14:09:12	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
6	14:09:05	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
7	14:08:58	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
8	14:08:51	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
9	14:08:44	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
10	14:08:37	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
11	14:08:30	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1

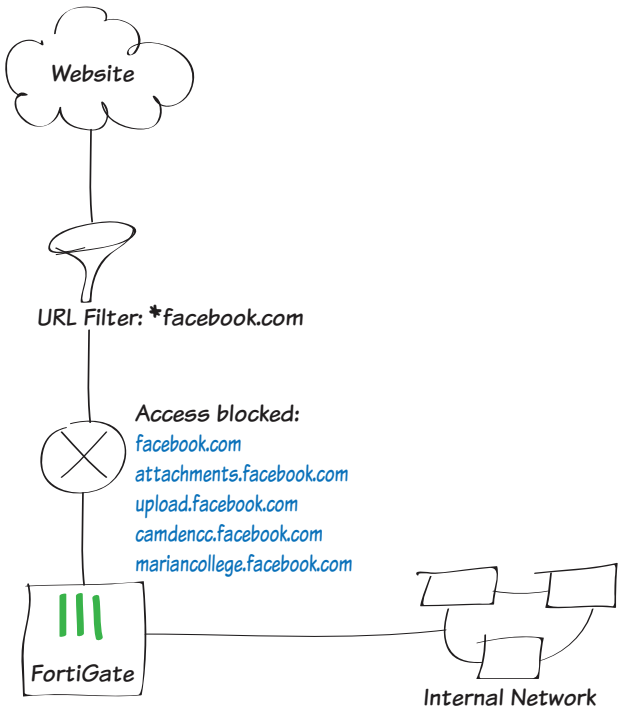
Watch the video

Blocking Facebook

When you allow access to a particular type of content, such as the FortiGuard Social Networking category, there may still be certain websites in that category that you wish to prohibit. In this example, you will learn how to configure a FortiGate to prevent access to a specific social networking website, including its subdomains, by means of a static URL filter. By using SSL inspection, you ensure that this website is also blocked when accessed through HTTPS protocol.

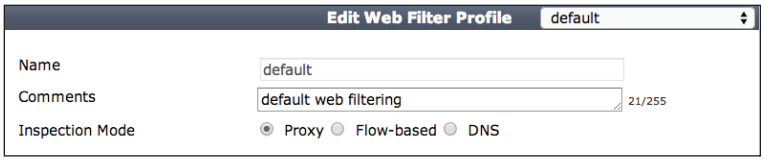
This recipe requires an active FortiGuard web filtering subscription

1. Editing the Web FIter profile
2. Verifying the SSL inspection profile
3. Creating a security policy
4. Results

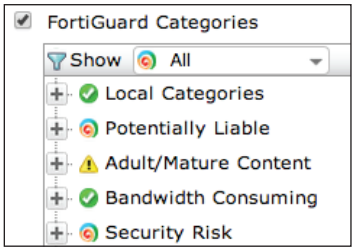


1. Editing the Web Filter profile

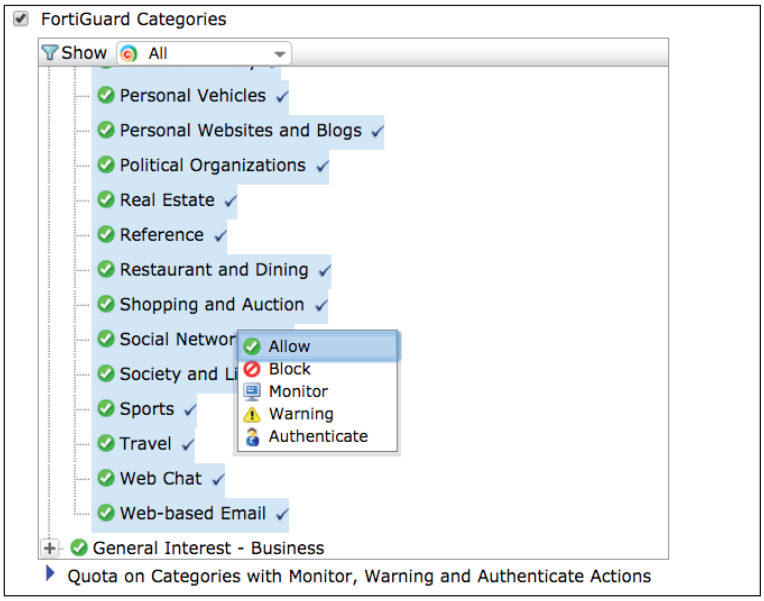
Go to **Security Profiles** > **Web Filter** and edit the default Web Filter profile. Set **Inspection Mode** to **Proxy**.



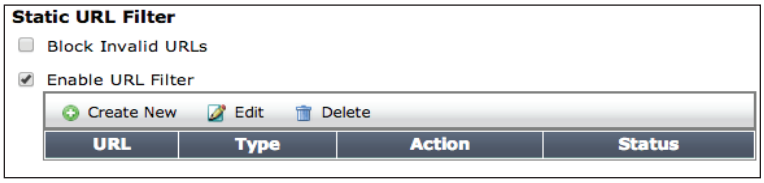
Enable the **FortiGuard Categories** that allow, block, monitor, warn, or authenticate websites, depending on the type of content.



Under FortiGuard Categories, go to **General Interest - Personal**. Right-click on the **Social Networking** subcategory and ensure it is set to **Allow**.



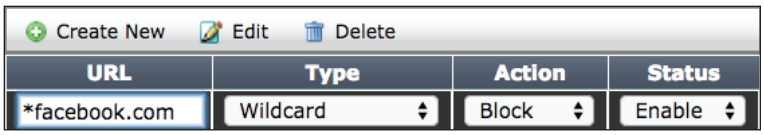
To prohibit visiting one particular social networking site in that category, go to **Static URL Filter**, select **Enable URL Filter**, and then click **Create New**.



For your new web filter, enter the URL of the website you are attempting to block. If you want to block all the subdomains of that website, omit the protocol in the URL and enter an asterisk (*). For this example, enter:

```
*facebook.com
```

Set **Type** to **Wildcard**, set **Action** to **Block**, and set **Status** to **Enable**.

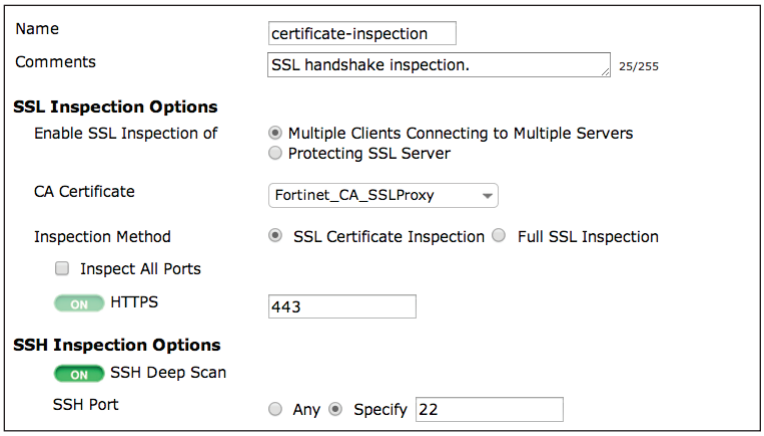


2. Verifying the SSL inspection profile

Go to **Policy & Objects > Policy > SSL Inspection** and edit the **certificate-inspection** profile.

Ensure that **CA Certificate** is set to the default **Fortinet_CA_SSLProxy**.

Ensure **Inspection Method** is set to **SSL Certificate Inspection** and **SSH Deep Scan** is set to **ON**.

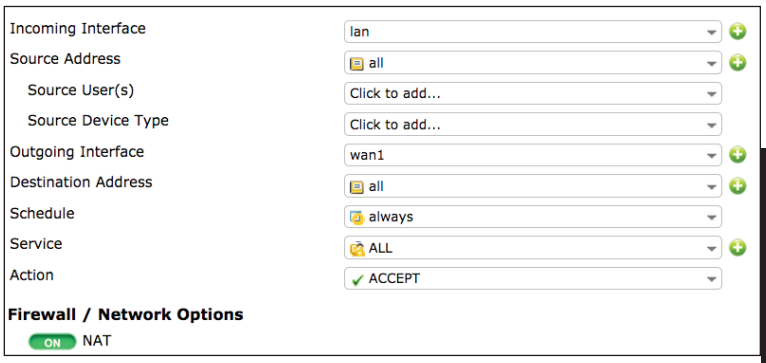


3. Creating a security policy

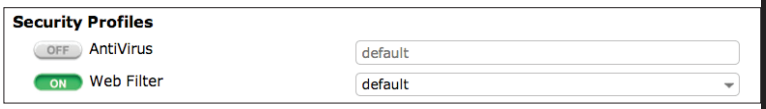
Go to **Policy & Objects > Policy > IPv4**, and click **Create New**.

Set the **Incoming Interface** to allow packets from your internal network and set the **Outgoing Interface** to proceed to the Internet-facing interface (typically **wan1**).

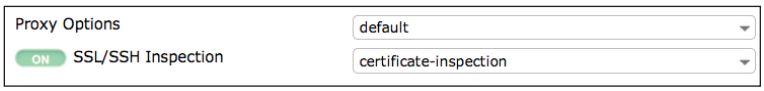
Enable **NAT**.



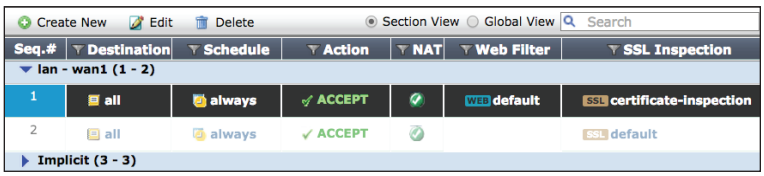
Under **Security Profiles,** enable **Web Filter** and select the **default** web filter.



This automatically enables **SSL/ SSH Inspection**. Select **certificate-inspection** from the dropdown menu.



After you have created your new policy, ensure that it is at the top of the policy list. To move your policy up or down, click and drag the far left column of the policy.



4. Results

Visit the following sites to verify that your web filter is blocking websites ending in facebook.com:

- facebook.com
- attachments.facebook.com
- upload.facebook.com

A FortiGuard **Web Page Blocked!** page should appear.

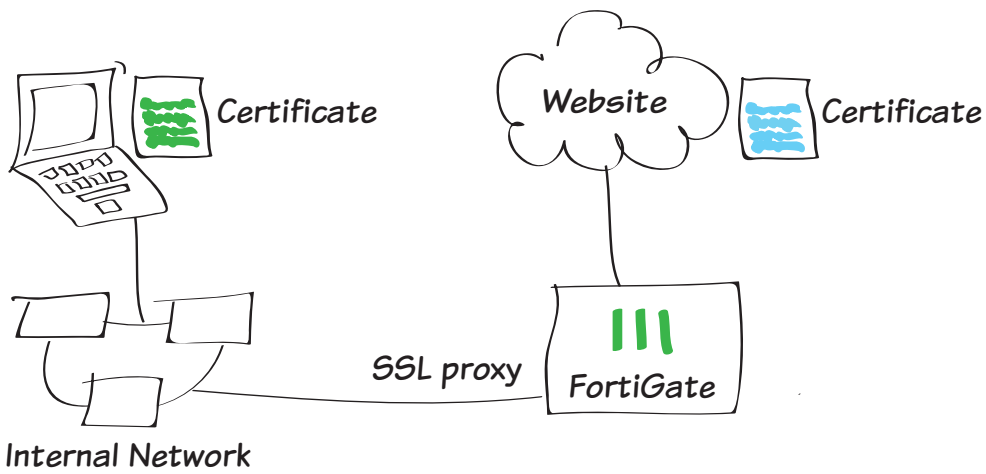
Visit https://www.facebook.com to verify that HTTPS protocol is blocked. A **Web Page Blocked!** page should appear.

Watch the video

Preventing certificate errors

This example illustrates how to prevent your users from getting a security certificate warning when you have enabled full SSL inspection (also called deep inspection).

A bad habit that many users have is selecting **Continue** when they receive a warning. Instead of encouraging this practice, you can use the examples below to prevent certificate warnings from appearing: Using the default FortiGate certificate or using a custom certificate.



Using the default FortiGate certificate

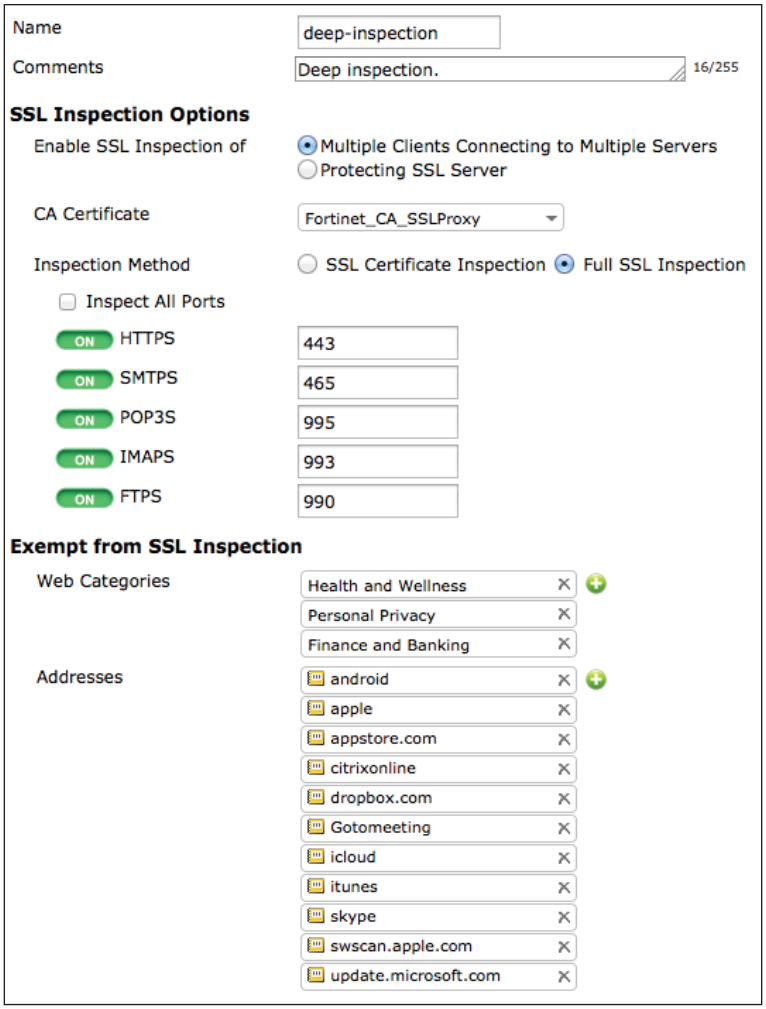
All FortiGates have a default certificate that is used for SSL deep inspection. This certificate is also used in the default deep-inspection profile.

To prevent your users from seeing certificate warnings you can distribute this certificate to your user's devices.

1. Viewing the deep-inspection SSL profile

Go to **Policy & Objects > SSL/ SSH Inspection** and edit the **deep-inspection** profile.

In this policy, the web categories **Health and Wellness**, **Personal Privacy**, and **Finance and Banking** are excluded from SSL inspection by default. Applications that require unique certificates, such as iTunes and Dropbox, have also been excluded.



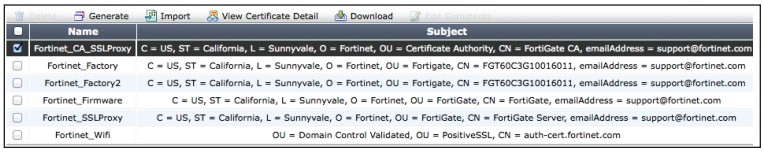
2. Enabling certificate configuration in the web-based manager

Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply**.

3. Downloading the Fortinet_CA_SSLProxy certificate

Go to **System > Certificates > Local Certificates** to download the Fortinet_CA_SSLProxy certificate.

Make the CA certificate file available to your users by checkmarking the box next to the certificate name.



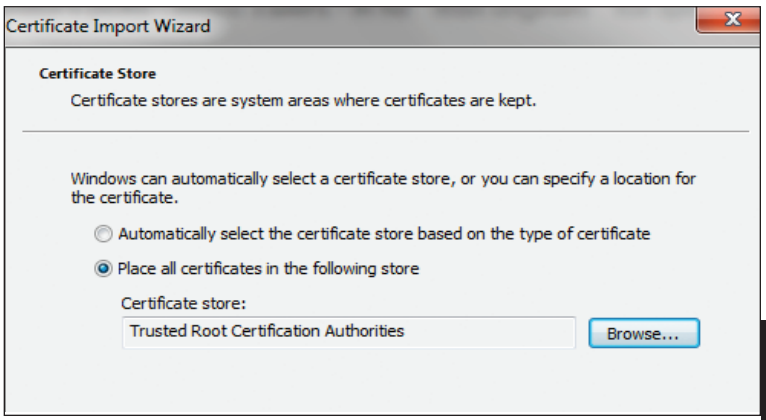
4. Importing the CA certificate into the web browser

Internet Explorer:

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates** and find the **Trusted Root Certification Authorities**.

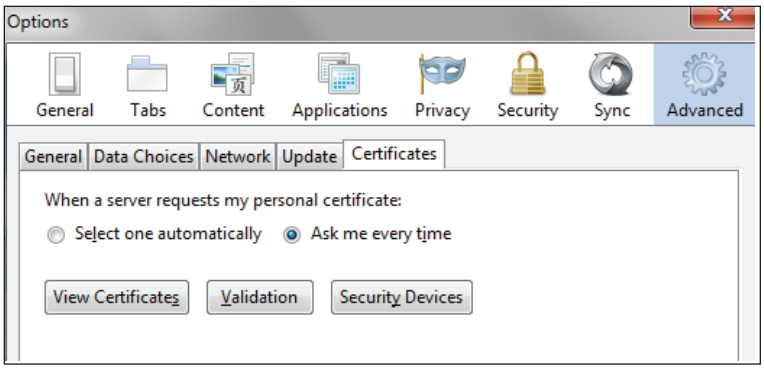
Import the certificate using the Import Wizard. Make sure that the certificate is imported into Trusted Root Certification Authorities.

You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.

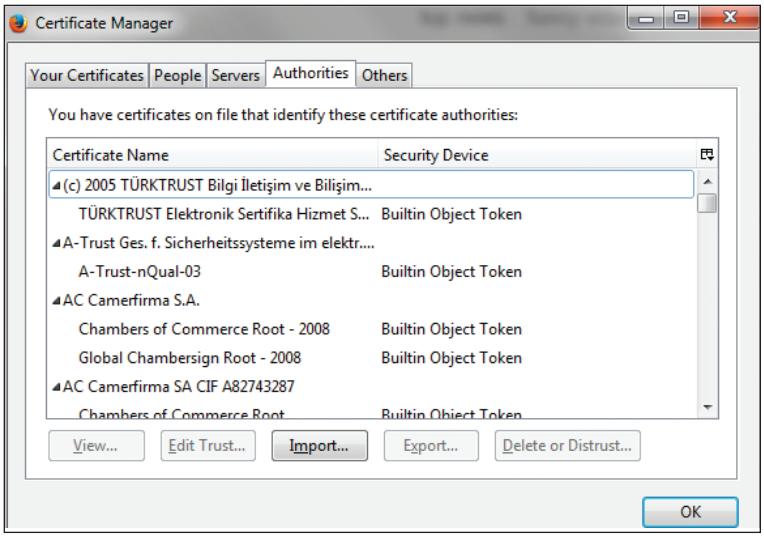


Firefox:

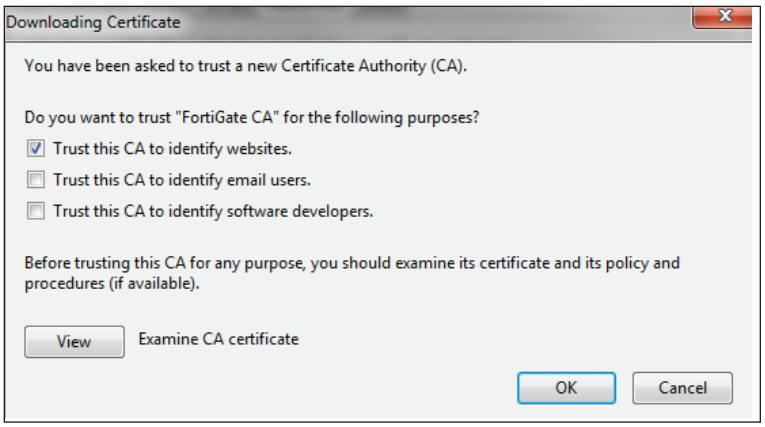
Depending on the platform, go to **Menu > Options or Preferences > Advanced** and find the **Certificates** tab.



Click **View Certificates**, specifically the **Authorities** certificate list

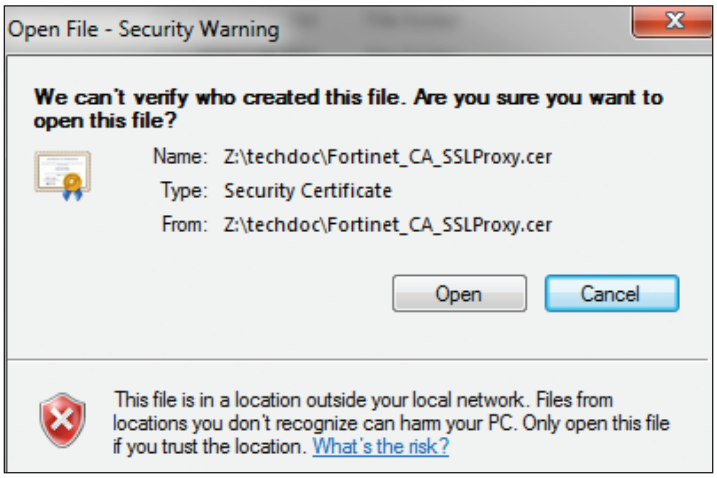


Click **Import** and select the Fortinet_CA_SSLProxy certificate file.



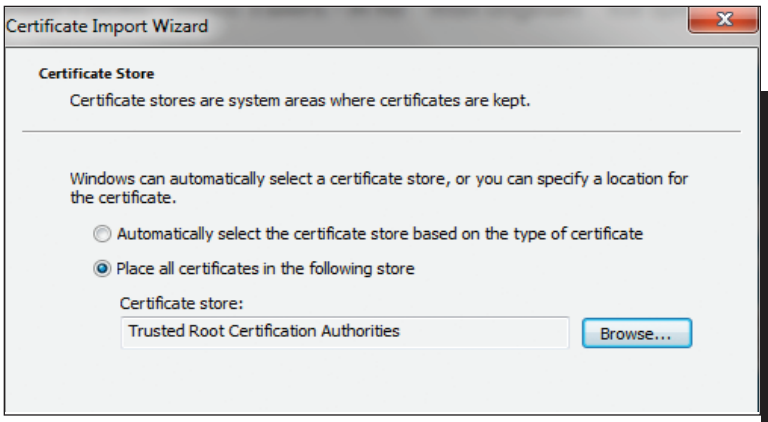
Google Chrome and Safari:

Locate and open the downloaded Fortinet_CA_SSLProxy certificate file. Choose **Open** and click **Install Certificate**. The Import Wizard appears.



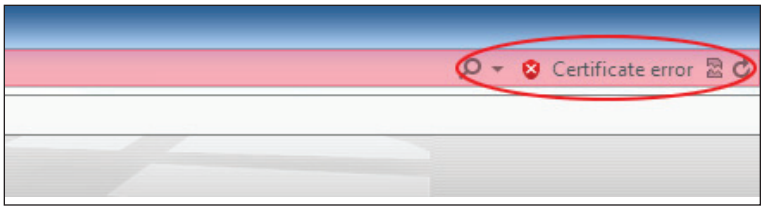
Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

You will see a warning because the FortiGate unit's certificate is self signed. It is safe to select **Yes** to install the certificate.



5. Results

Before installing the FortiGate SSL CA certificate, even if you bypass the error message by selecting **Continue to this website**, the browser may still show an error in the toolbar.



After you install the FortiGate SSL CA certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection. iTunes will also be able to run without a certificate error.

Watch the video

Using a custom certificate

In this method, a custom certificate is first signed by a recognized third-party CA and then installed on the FortiGate. This results in a chain of trust that does not exist when the FortiGate's default certificate is used. This example allows network users to trust the FortiGate as a CA in its own right. Once the FortiGate is trusted, your users will no longer see certificate errors.

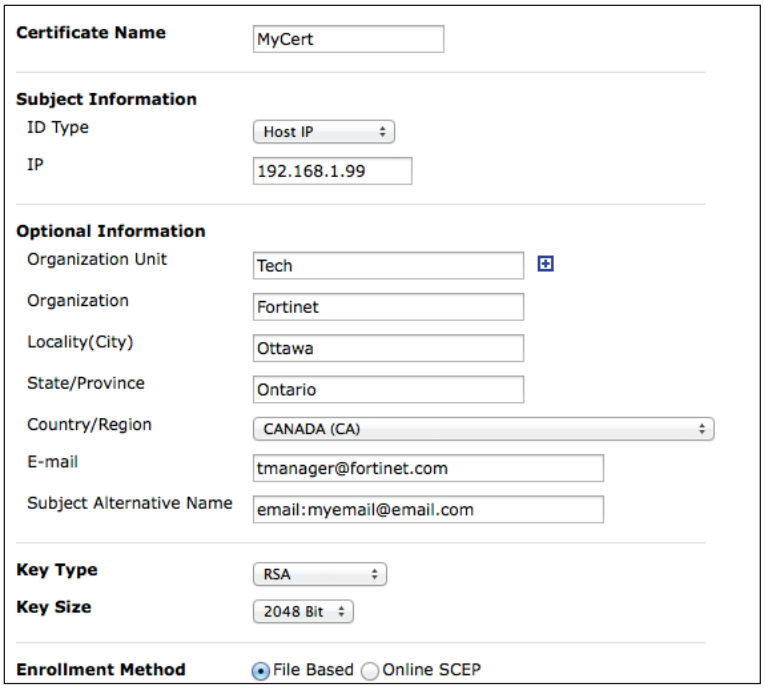
1. Generating a certificate signing request (CSR)

Go to **System > Certificates > Local Certificates** and select **Generate**.

In the **Generate Certificate Signing Request** page, fill out the required fields. You can enter a maximum of five **Organization Units**.

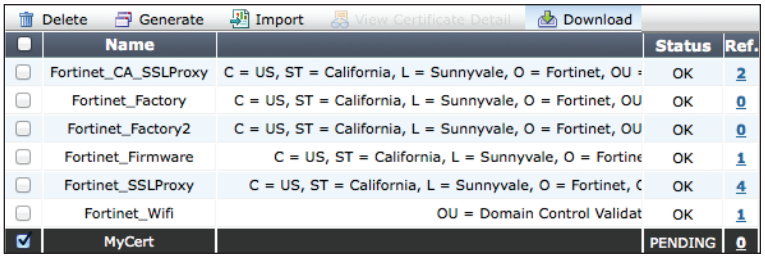
You may enter **Subject Alternative Names** for which the certificate is valid. Separate the names using commas.

To ensure PKCS12 compatibility, do not include spaces in the certificate name.



Go to **System > Certificates > Local Certificates** to view the certificate list. The status of the CSR created will be listed as **Pending.** Select the certificate and click **Download**.

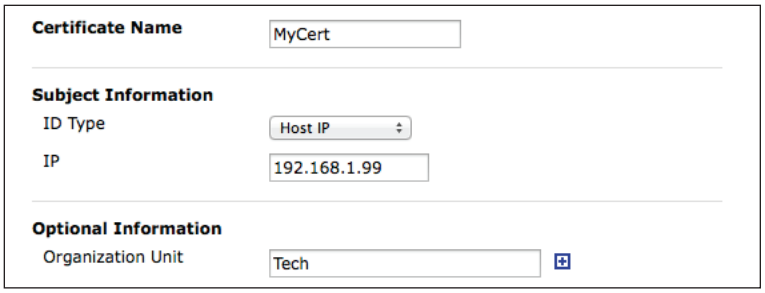
This CSR will need to be submitted and signed by an enterprise root CA before it can be used. When submitting the file, ensure that the template for a **Subordinate Certification Authority** is used.



2. Importing a signed server certificate from an enterprise root CA

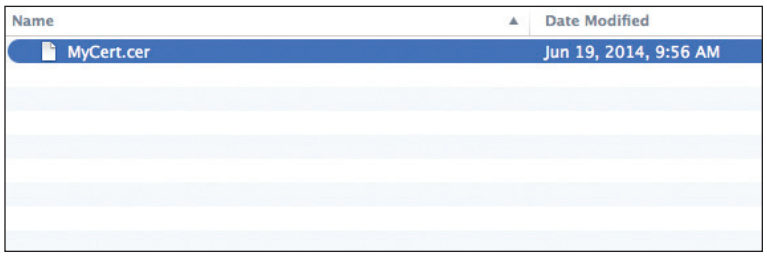
Once the CSR is signed by an enterprise root CA, you can import it into the FortiGate unit.

Go to **System > Certificates > Local Certificates** and click **Import**. From the **Type** drop down menu select **Local Certificate** and click **Choose File**.



Locate the certificate you wish to import, select it, and click **Open**.

The CA signed certificate will now appear on the **Local Certificates** list.

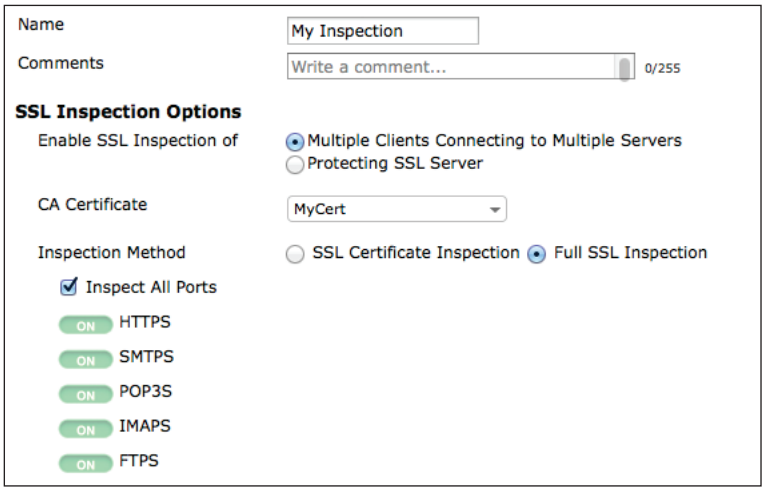


3. Creating an SSL inspection profile

To use your certificate in an SSL inspection profile go to **Policy & Objects > Policy > SSL/SSH Inspection**.

Create a new **SSL Inspection Profile**. In the **CA Certificate** drop down menu, select the certificate you imported. Set the **Inspection Method** to **Full SSL Inspection** and **Inspect All Ports**.

You may also need to select web categories and addresses to be exempt from SSL inspection.

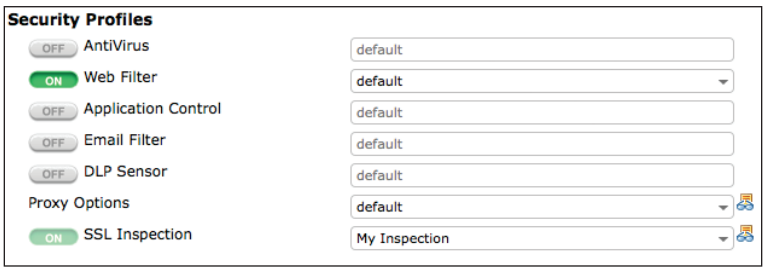


If the certificate does not appear in the list, verify that the template used to sign the certificate was for a CA and not simply for user or server identification.

4. Editing your Internet policy to use the new SSL inspection profile

Go to **Policy & Objects > Policy > IPv4** and edit the policy controlling Internet traffic.

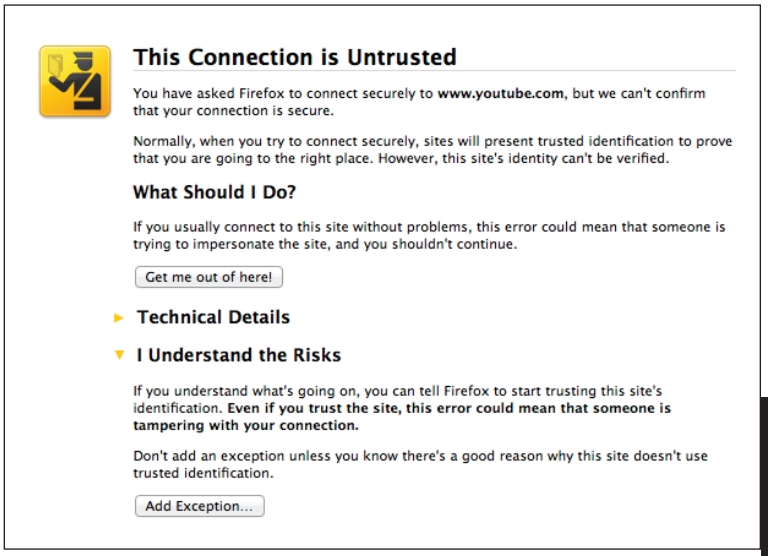
Under **Security Profiles**, ensure that **SSL Inspection** and **Web Filter** are **On**. From the **SSL Inspection** dropdown menu, select your new profile. The **Web Filter** can remain as **default**.



5. Results

When visiting an HTTPS website such as https://www.youtube.com/ a warning would normally appear if you were using a self-signed certificate.

If you have the correct type of certificate, signed by a recognized CA, warnings should no longer appear.



If you view the website's certificate information, the **Issued By** section should contain the information of your custom certificate, indicating that the traffic is subject to deep inspection.

Network users can now manually import the certificate into their trusted root CA certificate store (Internet Explorer and Chrome) and/or into their browsers (Firefox).

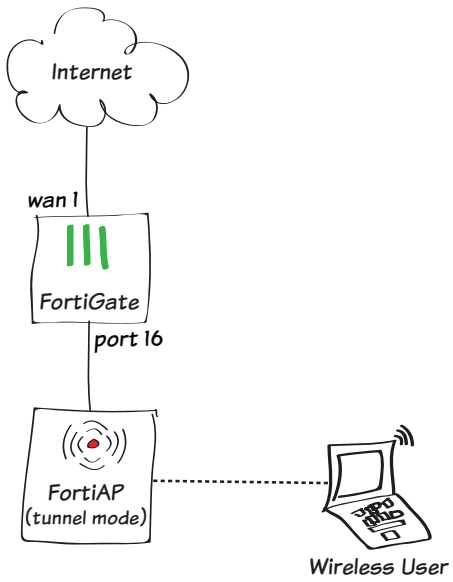
Alternately, if the users are members of a Windows domain, the domain administrator can use a group policy to force them to trust the self-signed certificate that the FortiGate is presenting.

Adding a WiFi network with a FortiAP

You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

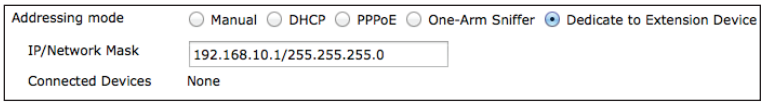
In this example, a FortiAP unit is connected to and managed by a FortiGate unit, allowing wireless access to the network.

1. Connecting and authorizing the FortiAP unit
2. Creating an SSID
3. Creating a custom FortiAP profile
4. Allowing wireless access to the Internet
5. Results



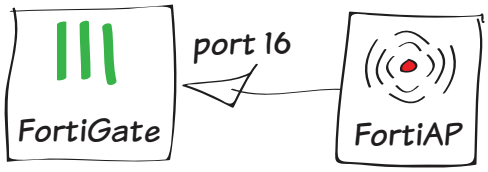
1. Connecting and authorizing the FortiAP unit

Go to **System > Network > Interfaces** and edit the interface that will connect to the FortiAP (in the example, port 16).

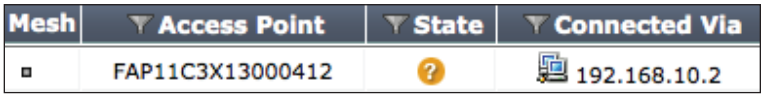


Set **Addressing Mode** to **Dedicate to Extension Device** and set an **IP/Network Mask**.

Connect the FortiAP unit to the interface.

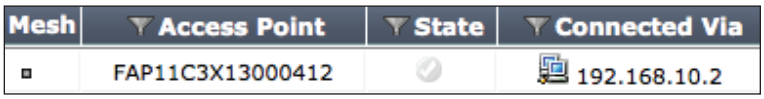


Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a beside it because the device is not authorized.



It may take a few minutes for the FortiAP to appear.

Highlight the FortiAP unit on the list and select **Authorize**. A is now shown beside the FortiAP, showing that it is authorized but not yet online.



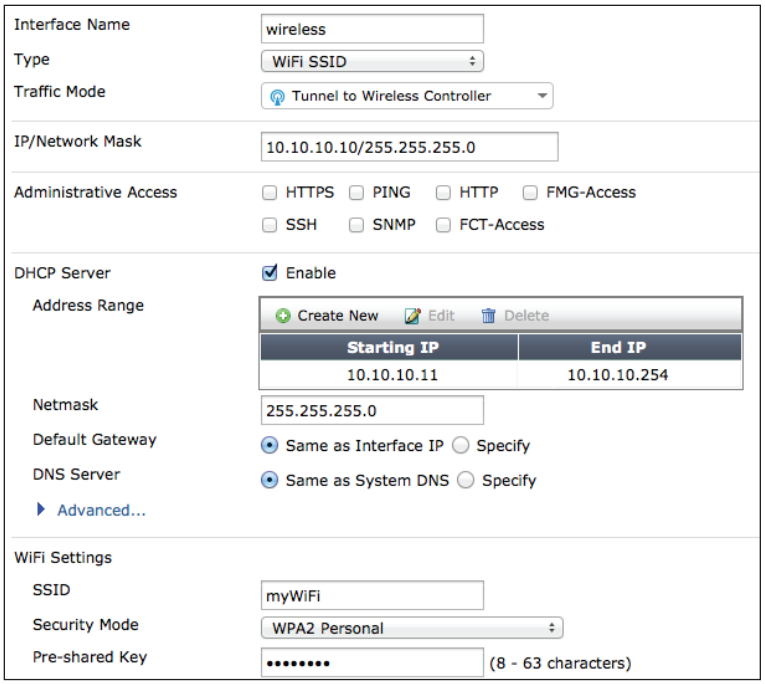
2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**.

Select an **IP/Network Mask** for the wireless interface and enable **DHCP Server**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

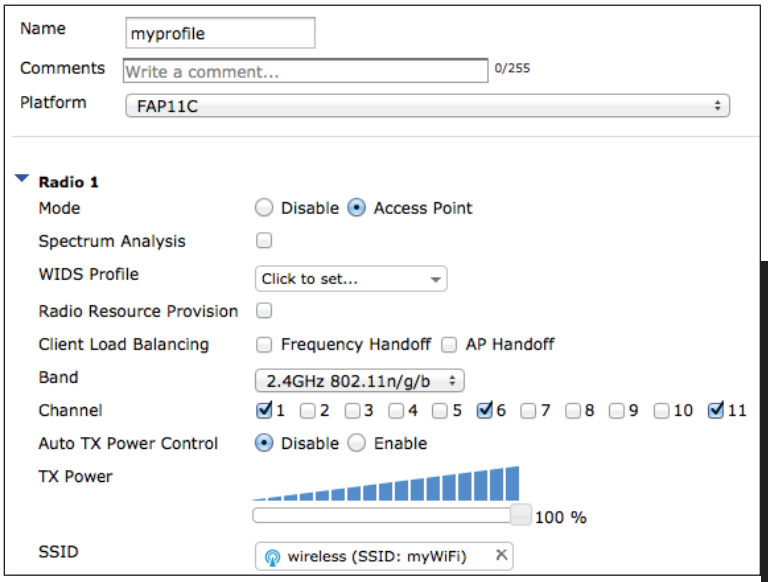


3. Creating a custom FortiAP profile

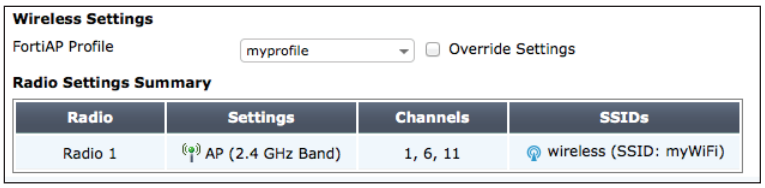
Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (in the example, FAP11C).

Set **SSID** to use the new SSID.



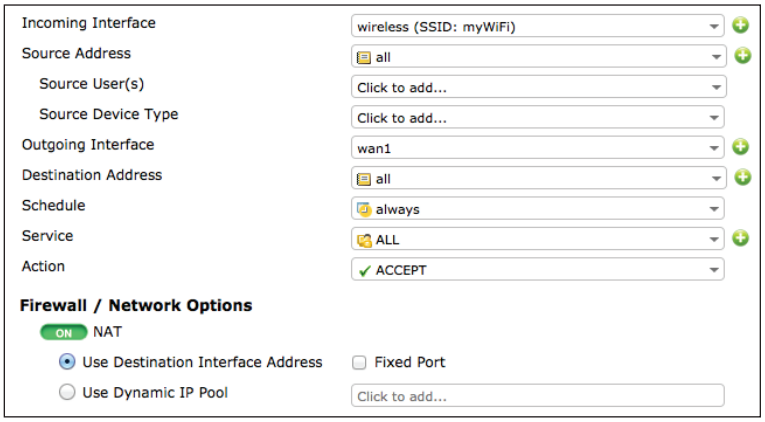
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. Edit the FortiAP and set **FortiAP Profile** to use the new profile.



4. Allowing wireless access to the Internet

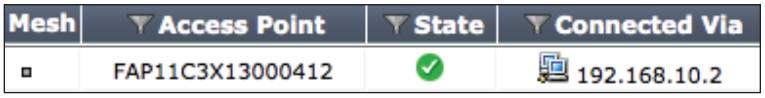
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the SSID and **Outgoing Interface** to your Internet-facing interface. Ensure that **NAT** is turned on.



5. Results

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A ✓ now appears beside the FortiAP, showing that the unit is authorized and online.



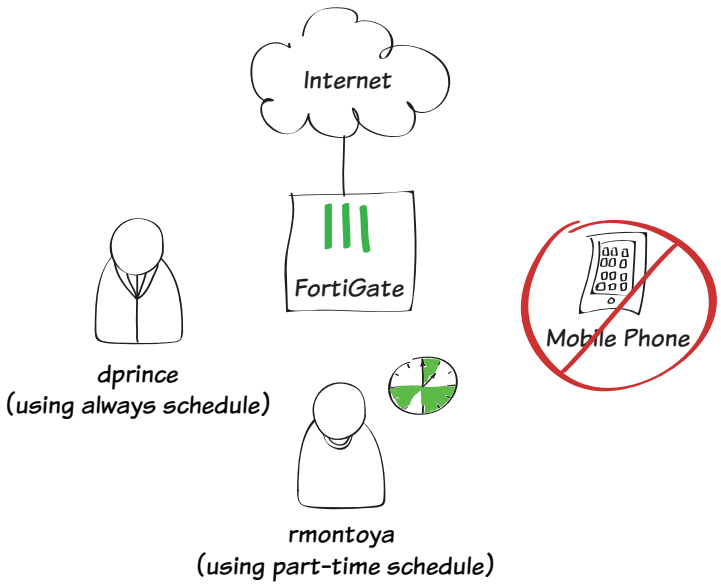
Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

User and device authentication

In this example, user authentication and device authentication provide different access for staff members based on whether they are full-time or part-time employees, while denying all traffic from mobile phones.

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN.

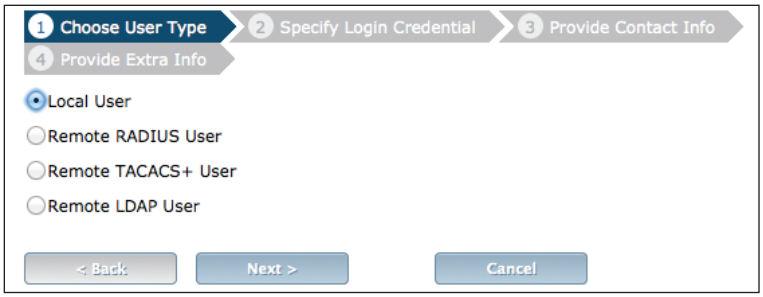
1. Defining two users and two user groups
2. Creating a schedule for part-time staff
3. Defining a device group for mobile phones
4. Creating a policy for full-time staff
5. Creating a policy for part-time staff that enforces the schedule
6. Creating a policy that denies mobile traffic
7. Results

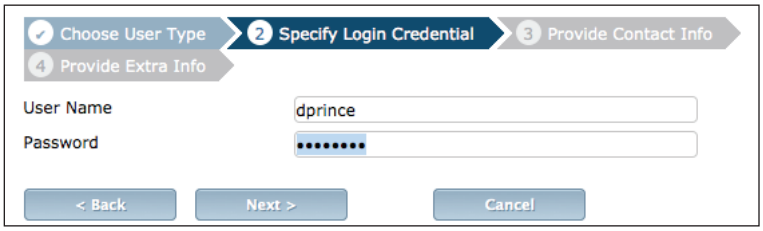


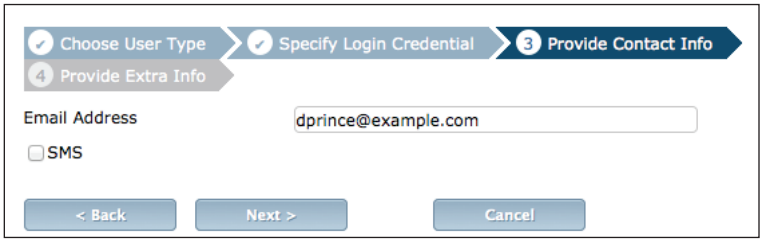
1. Defining two users and two user groups

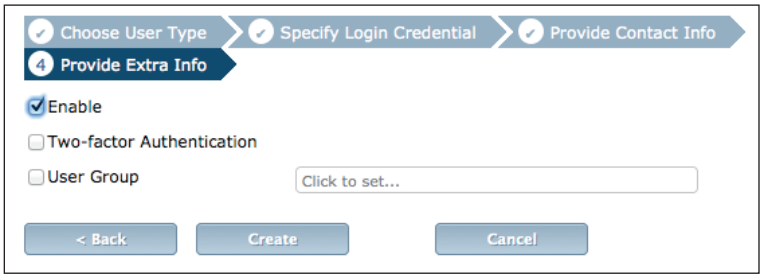
Go to **User & Device > User > User Definitions**.

Create two new users (in the example, *dprince* and *rmontoya*).







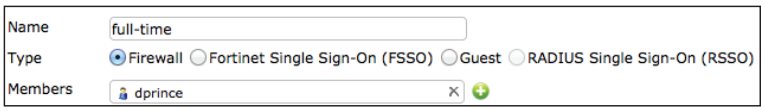


Both user definitions now appear in the user list.

User Name	Type	Two-factor Authentication	Ref.
dprince	LOCAL		0
guest	LOCAL		1
rmontoya	LOCAL		0

Go to **User & Device > User > User Groups**.

Create the user group *full-time* and add user *dprince.*

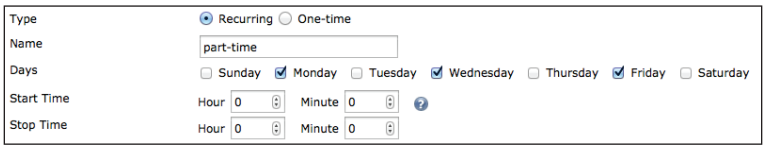


Create a second user group, *part-time*, and add user *rmontoya*.

2. Creating a schedule for part-time staff

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

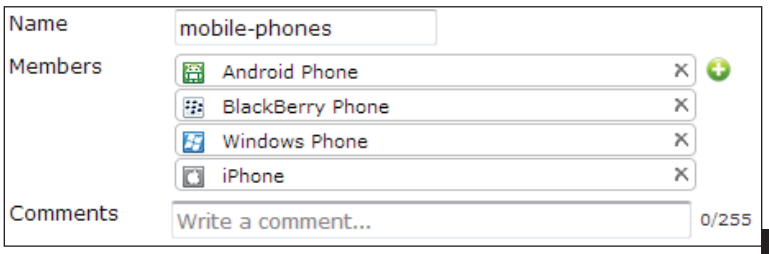
Set an appropriate schedule. In order to get results later, do not select the current day of the week.



3. Defining a device group for mobile phones

Go to **User & Device > Device > Device Groups** and create a new group.

Add the various types of mobile phones as **Members**.

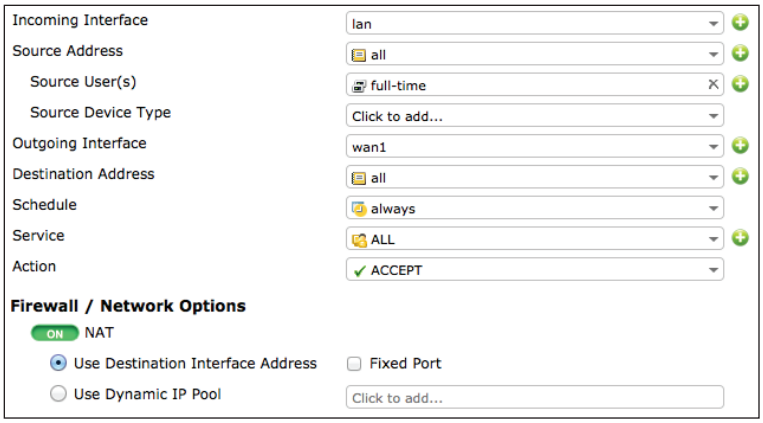


4. Creating a policy for full-time staff

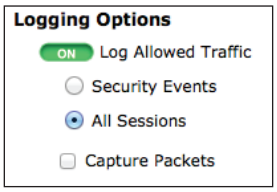
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the full-time group, **Outgoing Interface** to your Internet-facing interface, and ensure that **Schedule** is set to **always**.

Turn on **NAT**.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

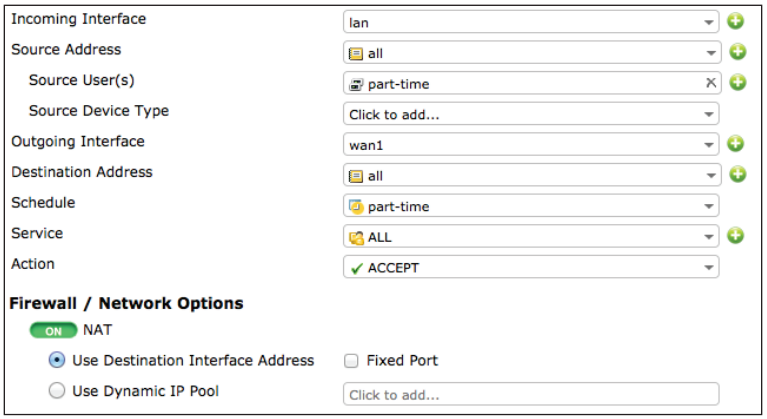


5. Creating a policy for part-time staff that enforces the schedule

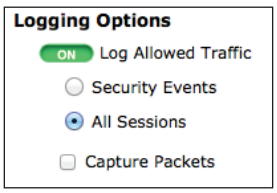
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the part-time group, **Outgoing Interface** to your Internet-facing interface, and set **Schedule** to use the part-time schedule.

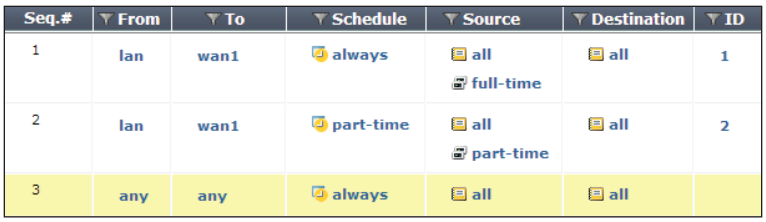
Turn on **NAT**.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



View the policy list. Click on the title row and select **ID** from the dropdown menu, then select **Apply**. Take note of the ID number that has been given to the part-time policy.



Seq.#	From	To	Schedule	Source	Destination	ID
1	lan	wan1	always	all full-time	all	1
2	lan	wan1	part-time	all part-time	all	2
3	any	any	always	all	all	

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console**, using the ID number of the part-time policy.

```
config firewall policy
   edit 2
      set schedule-timeout enable
   end
end
```

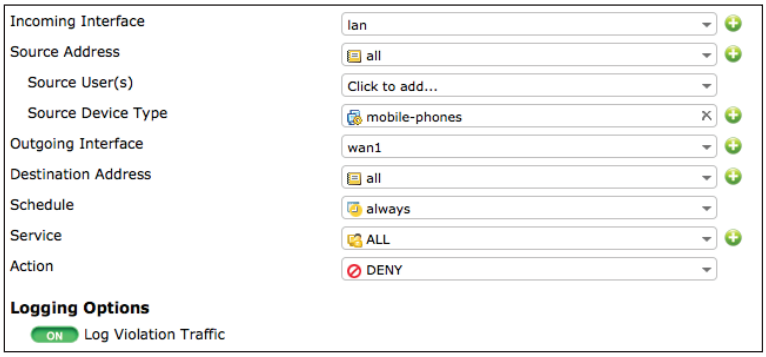
This will ensure that part-time users will have their access revoked during days they are not scheduled, even if their current session began when access was allowed.

6. Creating a policy that denies mobile traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source Device** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and set **Action** to **DENY**.

Leave **Log Violation Traffic** turned on.



Using a device group will automatically enable device identification on the local network interface.

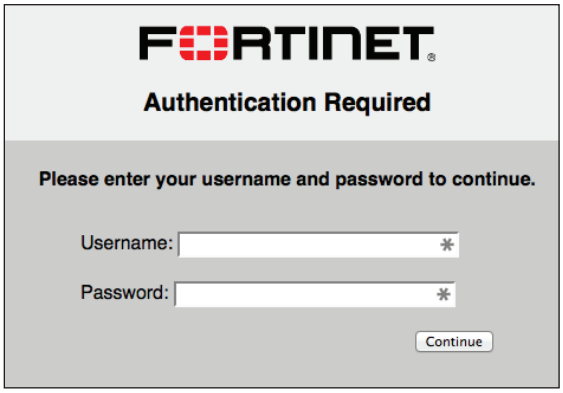
In order for this policy to be used, it must be located at the top of the policy list. Select any area in the far-left column of the policy and drag it to the top of the list.

Seq.#	From	To	Devices	Groups	Action
3	lan	wan1	Mobile Devices		DENY
1	lan	wan1		full-time	ACCEPT
2	lan	wan1		part-time	ACCEPT
4	any	any			DENY

7. Results

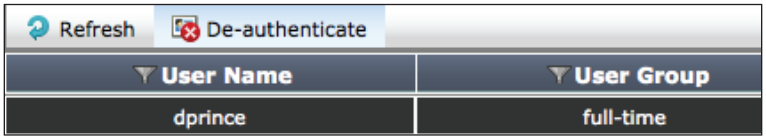
Browse the Internet using a computer. You will be prompted to enter authentication credentials.

Log in using the *dprince* account. You will be able to access the Internet at any time.

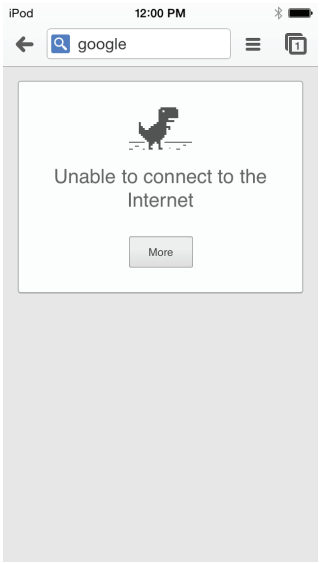


Go to **User & Device > Monitor > Firewall**. Highlight **dprince** and select **De-authenticate**.

Attempt to browse the Internet again. This time, log in using the *rmontoya* account. After authentication occurs, you will not be able to access the Internet.



Attempts to connect to the Internet using any mobile phone will also be denied.



You can view more information about the blocked and allowed sessions by going to **System > FortiView > All Sessions**.

Sessions that were blocked when you attempted to sign in using the *rmontoya* account will not have a user account shown in the **User** column.

Date/Time	User	Device	Destination	Action
09:10:21		iPhone	208.91.112.53	deny
09:10:21		Mac Mini	157.55.56.159	deny
09:10:21		Mac Mini	111.221.74.30	deny
09:10:21		Mac Mini	111.221.77.159	deny
09:10:21		iPhone	208.91.112.52	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:19		Mac Mini	157.55.56.159	deny
09:10:19		Mac Mini	157.56.52.30	deny
09:10:17		iPhone	208.91.112.52	deny
09:10:17	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:15	dprince	Mac Mini	64.94.107.34 (map-pb.quantserve.com.akadns.net)	accept
09:10:15	dprince	Mac Mini	174.36.240.82 (api.mixpanel.com)	accept

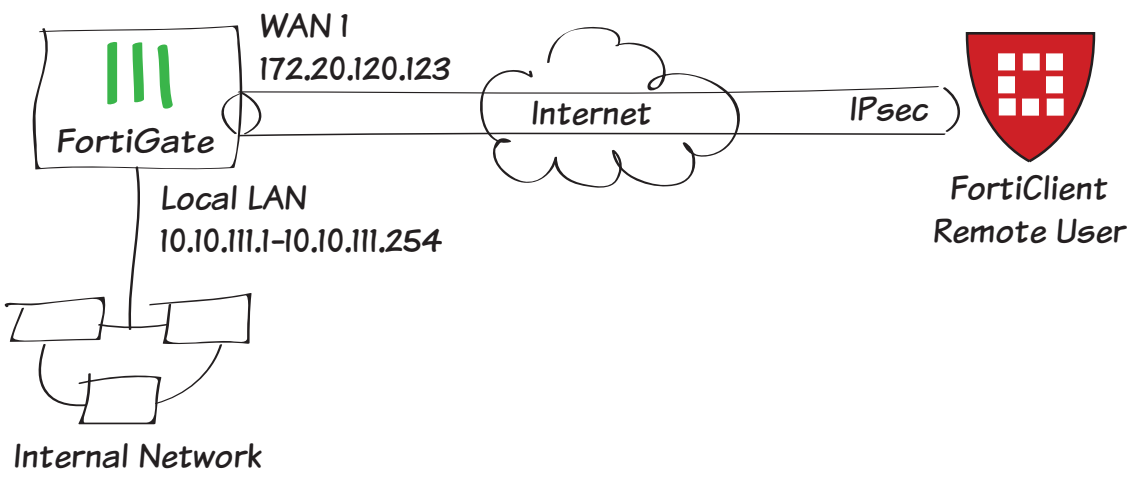
Watch the video

IPsec VPN for FortiClient

This recipe uses the IPsec VPN Wizard to provide a group of remote users with secure, encrypted access to the corporate network. The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet.

When the tunnel is configured, you will connect using the FortiClient application.

1. Creating a user group for remote users
2. Adding a firewall address for the local network
3. Configuring IPsec VPN using the IPsec VPN Wizard
4. Creating a security policy for access to the Internet
5. Configuring FortiClient
6. Results

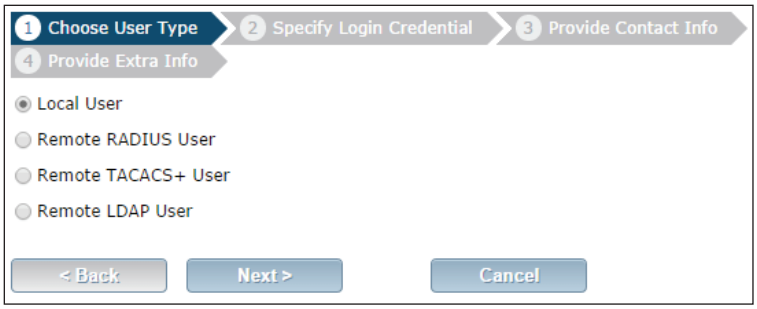


1. Creating a user group for remote users

Go to **User & Device > User > User Definition**.

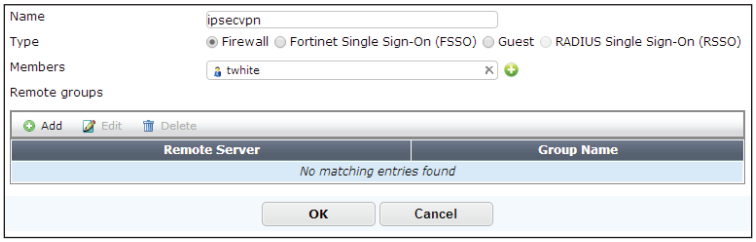
Create a new **Local User** with the User Creation Wizard.

Proceed through each step of the wizard, carefully entering the appropriate information.



Go to **User & Device > User > User Groups**.

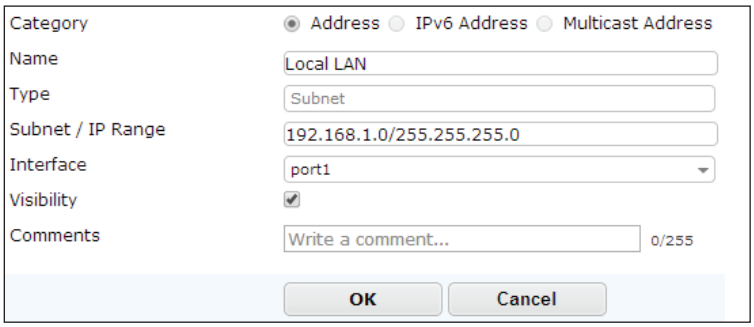
Create a user group for remote users and add the user you created.



2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add a firewall address for the Local LAN, including the subnet and local interface.

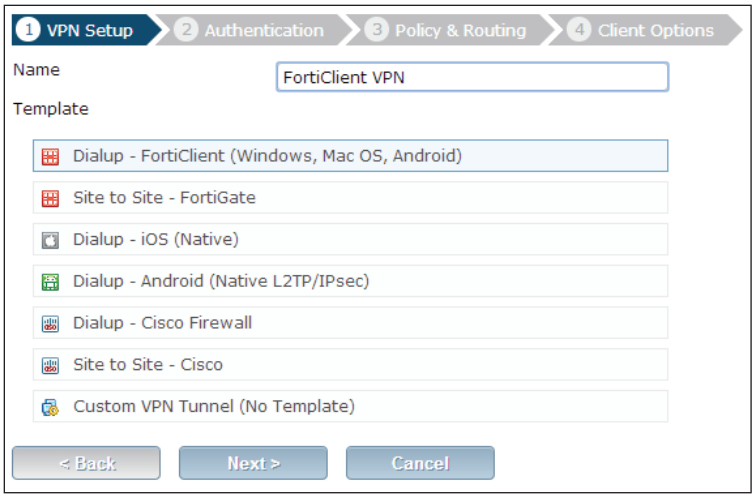


3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection, select **Dial Up - FortiClient (Windows, Mac OS, Android)**, and click **Next**.

The tunnel name must not have any spaces in it.

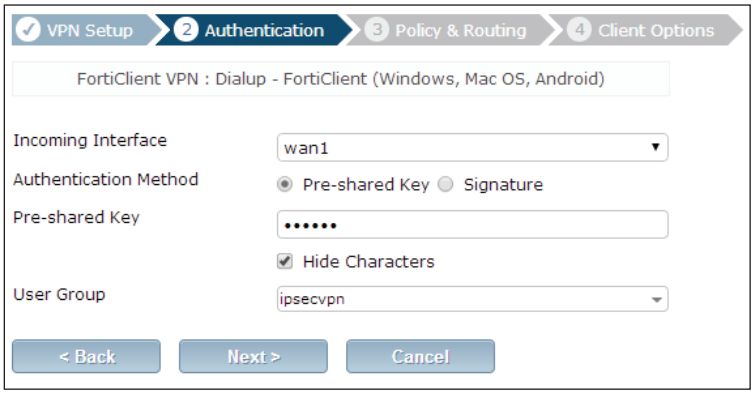


Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the 'ipsecvpn' user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.

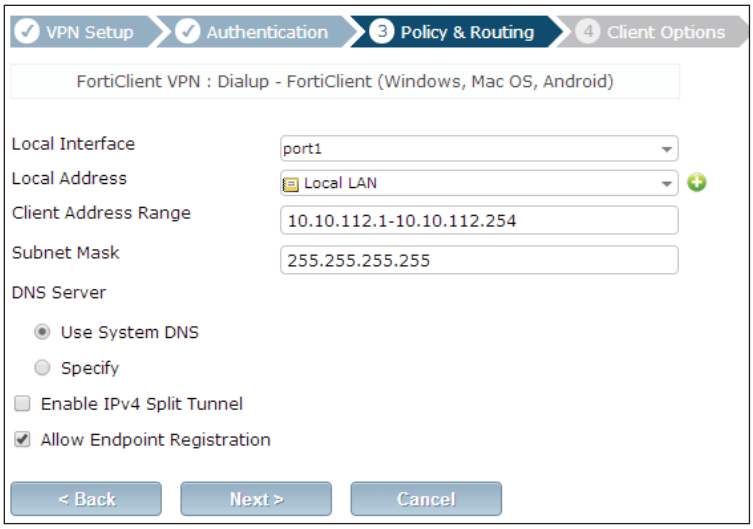


Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

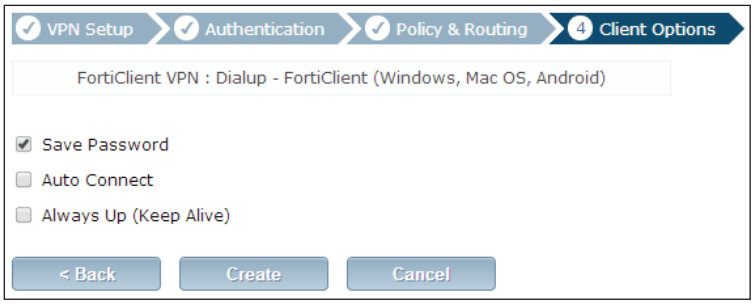
Enter an IP range for VPN users in the **Client Address Range** field.

The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **_range** suffix (in this case, **FortiClient VPN_range**).

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.



Click **Next** and select **Client Options** as desired.



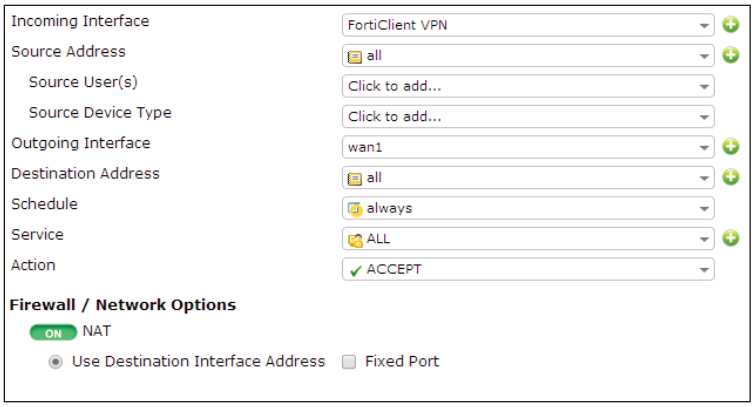
4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.

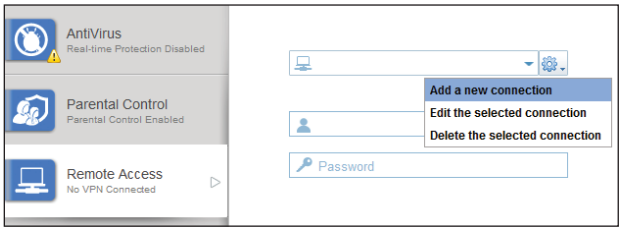
Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**. Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **all** and ensure that you enable **NAT**.



5. Configuring FortiClient

Open FortiClient, go to **Remote Access** and **Add a new connection**.

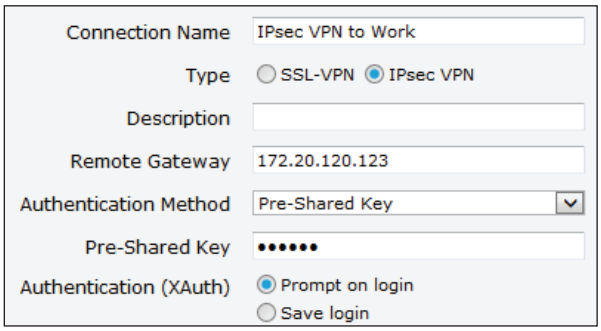


Provide a **Connection Name** and set the **Type** to **IPsec VPN**.

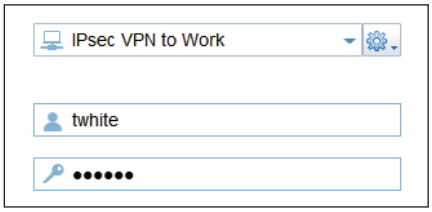
Set **Remote Gateway** to the FortiGate IP address.

Set **Authentication Method** to **Pre-Shared Key** and enter the key below.

Click **OK**.

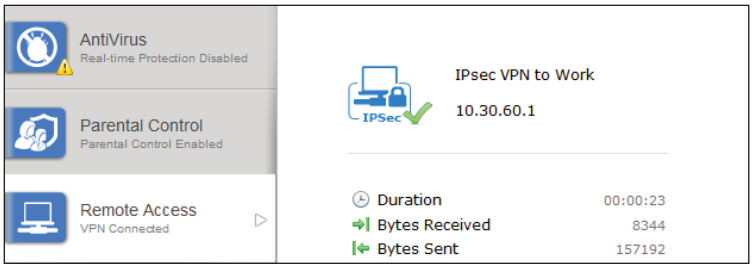


Select the new connection, enter the username and password, and click **Connect**.



6. Results

Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.

Name	Ty...	Remote Gatew...	Stat...	Incoming D...	Outgoing Data
iOSvpn_Native_0	Dialup	172.20.120.16	Up	9.22 K	3.48 K

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Verify that the **Sent/Received** column displays traffic successfully flowing through the tunnel.

Refresh Download Raw Log

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
4	11:21:42	port1		192.168.1.117	208.91.113.70	304 B / 304 B

Select an entry to view more information.

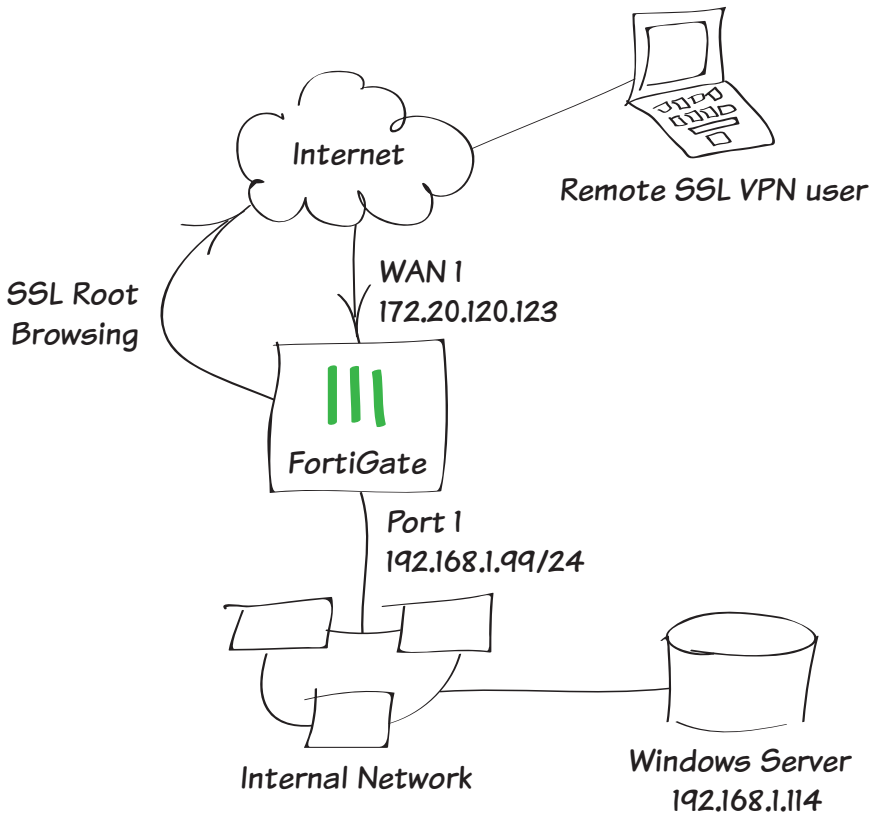
Dst	192.168.1.114	**Virtual Domain**	root
Received	72	**Source Country**	Reserved
Sent / Received	72 B / 72 B	**Duration**	63
Sent	72	**Application Details**	
Service	PING	**Protocol**	1

Watch the video

SSL VPN for remote users

This example provides remote users with access to the corporate network using SSL VPN and also connect to the Internet through the corporate FortiGate unit. During the connecting phase, the FortiGate unit will also verify that the remote user's antivirus software is installed and current.

1. Creating an SSL VPN portal for remote users
2. Creating a user and a user group
3. Adding an address for the local network
4. Configuring the SSL VPN tunnel
5. Adding security policies for access to the Internet and internal network
6. Setting the FortiGate unit to verify users have current AntiVirus software
7. Results



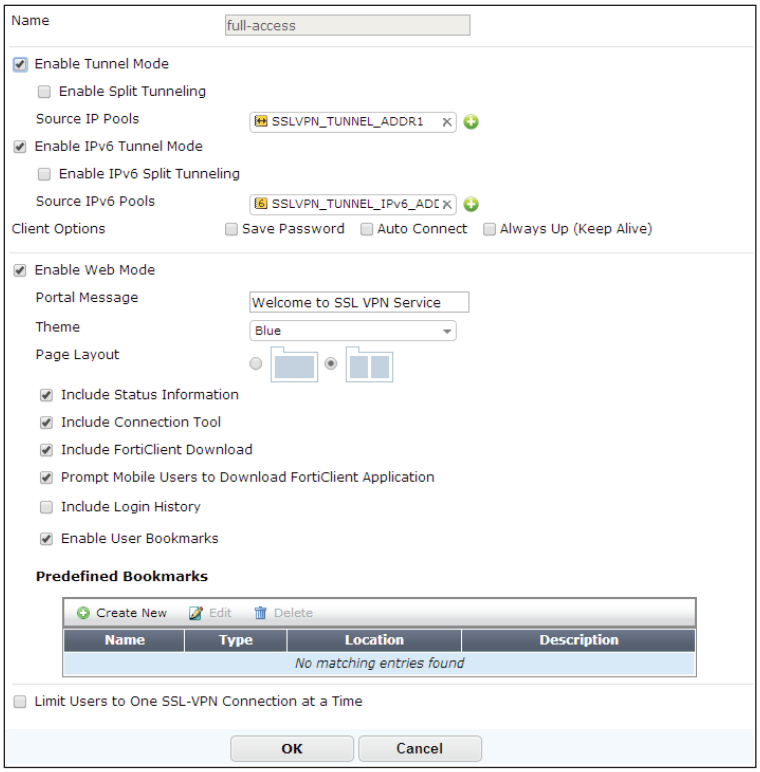
1. Creating an SSL VPN portal for remote users

Go to **VPN > SSL > Portals**.

Edit the full-access portal.

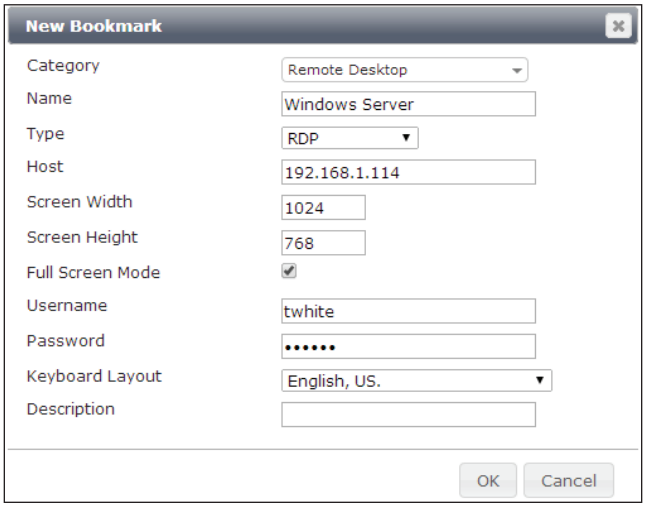
The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

Enable Split Tunneling is *not* enabled, so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.



Select **Create New** in the **Predefined Bookmarks** area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

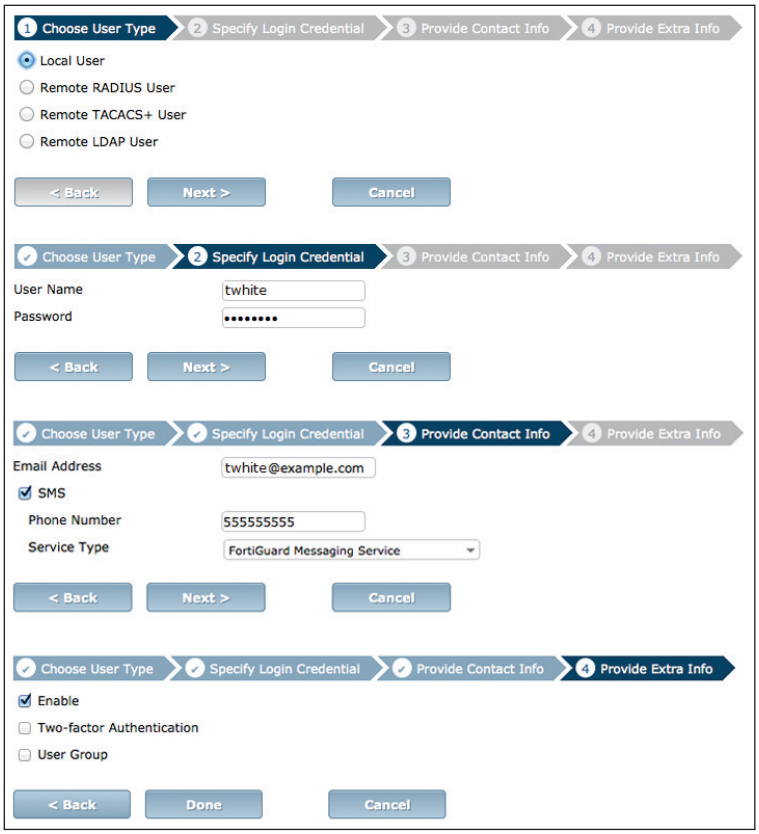


You must include a username and password. You will create this user in the next step, so be sure to use the same credentials.

2. Creating a user and a user group

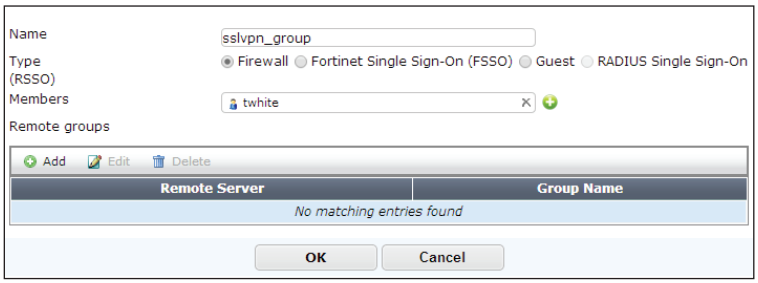
Go to **User & Device > User > User Definition**.

Add a remote user with the User Creation Wizard (in the example, ‘twhite’, with the same credentials used for the predefined bookmark).



Go to **User & Device > User > User Groups**.

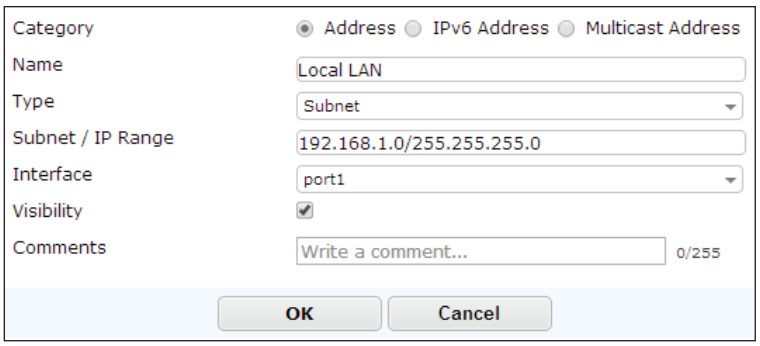
Add the user ‘twhite’ to a user group for SSL VPN connections.



3. Adding an address for the local network

Go to **Policy & Objects > Objects > Addresses**.

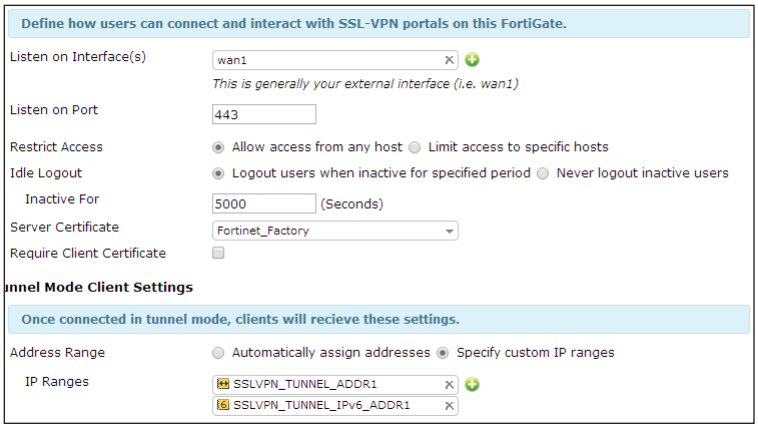
Add the address for the local network. Set **Subnet / IP Range** to the local subnet and set **Interface** to an internal port.



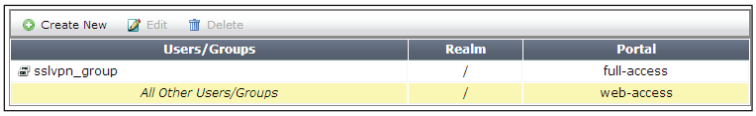
4. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **443** and **Specify custom IP ranges**.



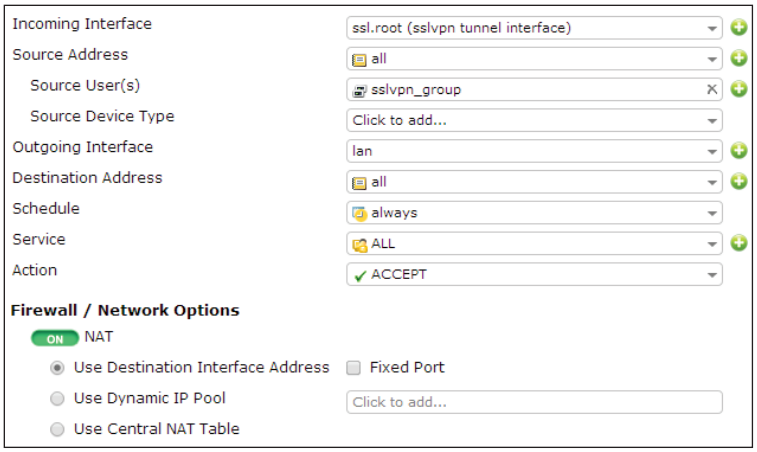
Under **Authentication/Portal Mapping**, add the SSL VPN user group.



5. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**.

Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.



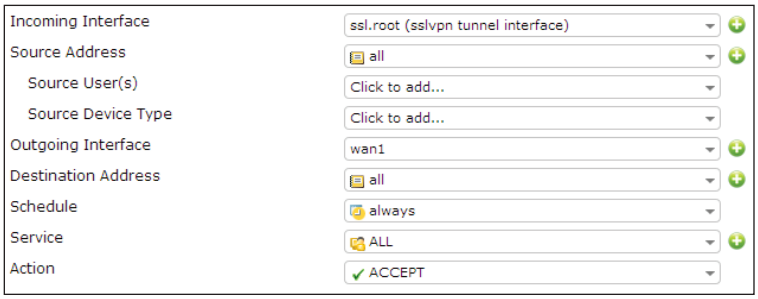
Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** group you created in step 2.

Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to **all**, enable **NAT**, and configure any remaining firewall and security options as desired.

Add a second security policy allowing SSL VPN access to the Internet.



For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

6. Setting the FortiGate unit to verify users have current AntiVirus software

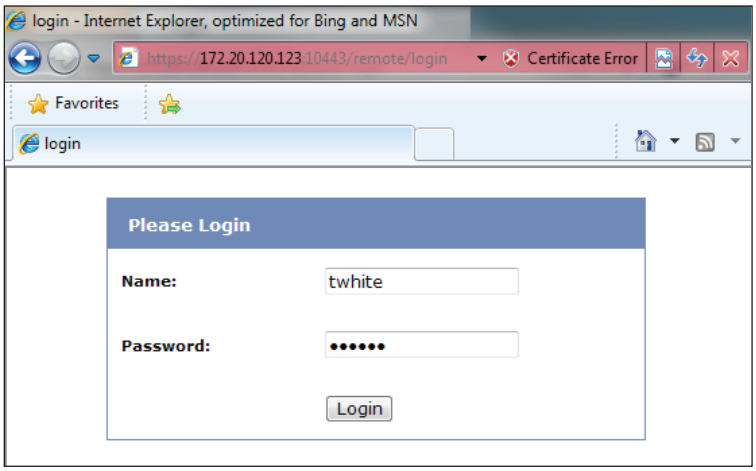
Go to **System > Status > Dashboard**.

In the **CLI Console** widget, enter the commands on the right to enable the host to check for compliant AntiVirus software on the remote user's computer.

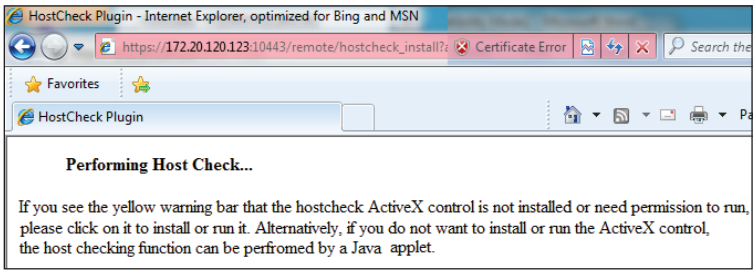
```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
```

7. Results

Log into the portal using the credentials you created in step 2.

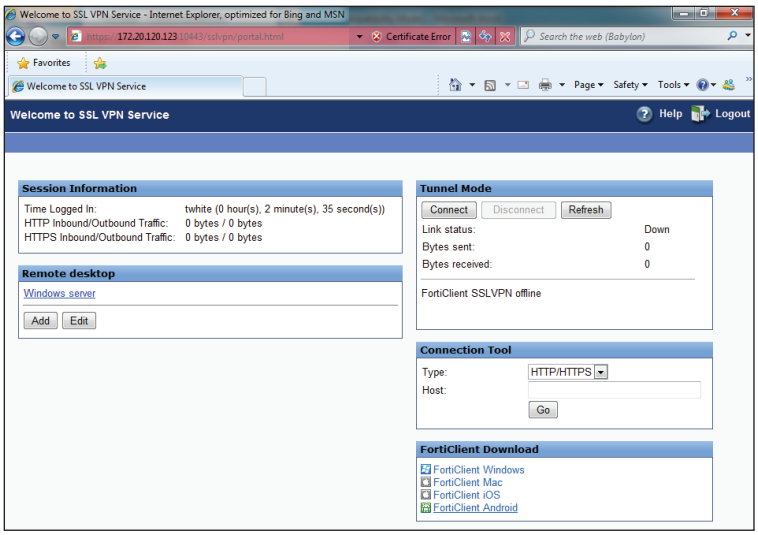


The FortiGate unit performs the host check.

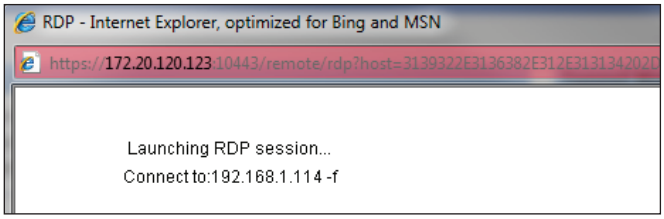


After the check is complete, the portal appears.

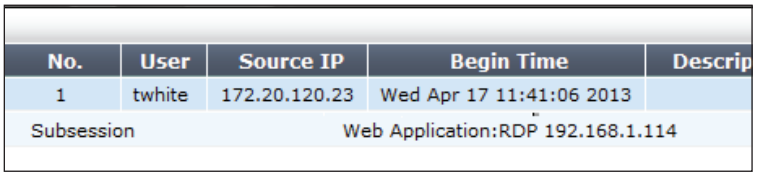
You may need to install the FortiClient application using the available download link.



Select the bookmark **Remote Desktop** link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

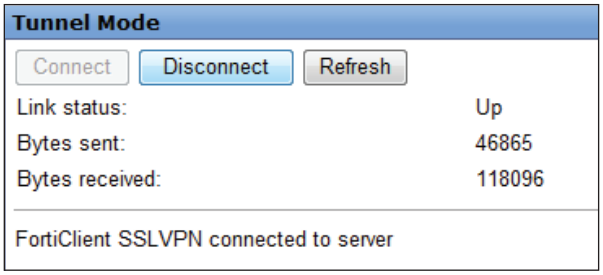


No.	User	Source IP	Begin Time	Descrip
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession			Web Application:RDP 192.168.1.114	

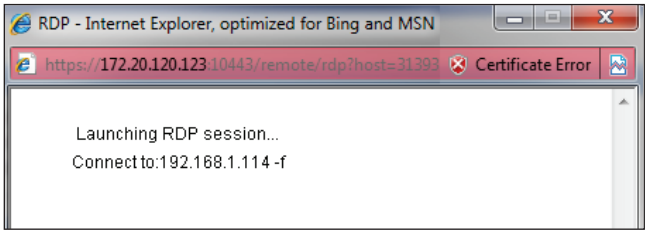
Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	**Virtual Domain**	root
Received	85591	**Source Country**	Reserved
Sent / Received	8.71 KB / 83.58 KB	**Duration**	36
Sent	8923	**Application Details**	
Group	N/A	**Service**	RDP
Protocol	6	**User**	twhite
Destination Country	Reserved	**Dst Port**	3389
roll	65389	**Status**	✓
Timestamp	Wed Apr 17 14:13:11 2013	**Tran Display**	noop
Sequence Number	2700	**Policy ID**	11
Src Interface	wan1	**Src**	twhite (172.20.120.23)
VPN	sslvpn_web_mode	**Sent Packets**	71
Level	notice	**VPN Type**	sslvpn
Src Port	53712	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	98	**Date/Time**	14:13:11 (Wed Apr 17 14:13:11 2013)
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.



Select the bookmark **Remote Desktop** link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.

No.	User	Source IP	Begin Time	D
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
	Subsession		Tunnel IP:10.212.134	

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	**Virtual Domain**	root
Received	326664	**Source Country**	Reserved
Sent / Received	54.36 KB / 319.01 KB	**Duration**	83
Sent	55665	**Application Details**	
Group	N/A	**Service**	RDP
Protocol	6	**User**	twhite
Destination Country	Reserved	**Dst Port**	3389
roll	65389	**Status**	✓
Timestamp	Wed Apr 17 14:17:15 2013	**Tran Display**	noop
Sequence Number	3618	**Policy ID**	11
Src Interface	wan1	**Src**	twhite (172.20.120.23)
VPN	sslvpn_web_mode	**Sent Packets**	329
Level	notice	**VPN Type**	sslvpn
Src Port	53820	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	407	**Date/Time**	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

Refresh Download Raw Log

#	Date/Time	Src Interface	Dst Interface	Src	Dst
1	14:26:05	ssl.root	wan1	10.212.134.200	74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	66.171.121.34 (fortinet.co
5	14:25:57	ssl.root	wan1	10.212.134.200	74.121.50.17 (www.pages
6	14:25:44	ssl.root	wan1	10.212.134.200	208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30

Watch the video

FortiGate System Administration Guide

The first steps in planning your configuration. Centralized management, tightening security, and best practices.
http://forti.net/admin

CLI Reference

Configuration of your device using the command line.
http://forti.net/cli

FortiOS Handbook

Definitive guide to configuring and operating FortiOS.
http://forti.net/handbook

Training Services

Course descriptions, availability, schedules, and locations of training programs in your area.
http://forti.net/training

QuickStart Guide Video

http://forti.net/vqsg